Number of Points on the Projective Curves

\[ aY^l = bX^l + cZ^l \] and \[ aY^{2l} = bX^{2l} + cZ^{2l} \] Defined over

Finite Fields, \( l \) an Odd Prime

N. Anuradha and S. A. Katre

University of Pune, Pune 411 007, India

E-mail: anuradha@math.unipune.ernet.in, sakatre@math.unipune.ernet.in

Communicated by A. C. Woods

Received March 8, 1997

The number of points on the curve \( aY^l = bX^l + cZ^l \) defined over a finite field \( \mathbb{F}_q \), where \( q \equiv 1 \pmod{e} \), is known to be obtainable in terms of Jacobi sums and cyclotomic numbers of order \( e \) with respect to this field. In this paper, we obtain explicitly the Jacobi sums and cyclotomic numbers of order \( e = l \) and \( e = 2l \) over finite fields \( \mathbb{F}_q \), where \( q \equiv 1 \pmod{e} \), for odd primes \( l \) and any prime \( p \) such that the order of \( p \) modulo \( l \) is even. Contrary to the case \( p \equiv 1 \pmod{e} \) considered in the literature, we have obtained these results solely in terms of \( q \) and \( l \). We apply these results to evaluate the number of \( \mathbb{F}_{q^n} \)-rational points on the non-singular projective curves \( aY^{l} = bX^{l} + cZ^{l} \) and \( aY^{2l} = bX^{2l} + cZ^{2l} \) defined over finite fields \( \mathbb{F}_q \), with conditions on \( q \), \( p \), and \( l \) as above. Using these evaluations, we obtain explicitly the \( \zeta \)-function of the former curve \( aY^l = bX^l + cZ^l \) defined over \( \mathbb{F}_q \) as a rational function in the variable \( t \). Thereby we corroborate the Weil conjectures (now theorems) for this concrete class of curves.

© 1999 Academic Press

1. INTRODUCTION

Let \( e \) be a positive integer \( >1 \) and let \( q \) be a positive integral power of a prime \( p \) such that \( q \equiv 1 \pmod{e} \). Let \( \mathbb{F}_q \) be a finite field of \( q \) elements and let \( \gamma \) be a generator of the cyclic group \( \mathbb{F}_q^* \). Let \( \zeta \) be a primitive (complex) \( e \)-th root of unity. Define a character \( \chi \) on \( \mathbb{F}_q^* \) by \( \chi(\gamma) = \zeta \) and set \( \chi(0) = 0 \).

Also set \( \chi'(0) = 0 \) for any integer \( i \). (Note that \( \chi'(v) = 1 \) for \( v \in \mathbb{F}_q^* \).)

For \( i, j \) modulo \( e \) (or for \( 0 \leq i, j \leq e - 1 \)), the Jacobi sums \( J(i, j) \) and the cyclotomic numbers \( A(i, j) \) of order \( e \) over \( \mathbb{F}_q \) are defined as

\[
J(i, j) = \sum_{v \in \mathbb{F}_q} \chi'(v) \chi'(v + 1) = \sum_{v \in \mathbb{F}_q \setminus \{0, -1\}} \zeta^{i \text{ind}_e(v) + j \text{ind}_e(v + 1)},
\]

where \( \text{ind}_e(v) \) denotes the multiplicative order of \( v \) modulo \( e \).
and

\[ A_{(i, j)_e} = \text{cardinality of } X_{(i, j)_e}, \]

where

\[ X_{(i, j)_e} = \{ v \in F_q^e | \chi(v) = \zeta^i, \chi(v + 1) = \zeta^j \} \]
\[ = \{ v \in F_q^e \setminus \{0, -1\} | \text{ind}_e(v) \equiv i (\text{mod } e), \text{ind}_e(v + 1) \equiv j (\text{mod } e) \}. \]

It is important to note that the sums \( J_d(i, j) \) and the numbers \( A_{(i, j)_e} \) are defined with respect to the character \( \chi: \gamma \mapsto \zeta \) on \( F_q^e \). In particular, they depend on the generator \( \gamma \) chosen. However, the numbers \( A_{(i, j)_e} \) do not depend upon \( \zeta \) whereas the sums \( J_d(i, j) \) may or may not depend on \( \zeta \); in general, \( J_d(i, j) \) is an element of the ring \( \mathbb{Z}[[\zeta]] \) for each \( i, j \) (mod \( e \)).

With respect to such a character \( \chi \) on \( F_q^e \), the Jacobi sums and the cyclotomic numbers of order \( e \) are related by

\[ \sum_{i=0}^{e-1} \sum_{j=0}^{e-1} \zeta^{-(a+b)} J_d(i, j) = e^2 A_{(a, b)_e} \quad \text{and} \quad \sum_{i=0}^{e-1} \sum_{j=0}^{e-1} A_{(i, j)_e} \zeta^{a+b} = J_d(a, b). \]

Thus knowing all the Jacobi sums, we know all the cyclotomic numbers, and the converse. Note that upon changing the generator of \( F_q^e \), the set of \( e^2 \) Jacobi sums newly obtained is a permutation of the initial set of Jacobi sums, and similarly this is true for the sets \( X_{(i, j)_e} \) and the cyclotomic numbers \( A_{(i, j)_e} \). In particular, if \( \gamma \) and \( \gamma' = \gamma^h \) are two generators of \( F_q^e \), there exists an integer \( h \) such that \( kh \equiv 1 \) (mod \( e \)) and one sees that

\[ J_d(i, j)_{\gamma'} = J_d(iy', jy'), \quad \sigma_{\gamma'}(J_d(i, j)) = J_d(i, j)_{\gamma}, \]
\[ (X_{(i, j)_e})_{\gamma'} = (X_{(ih, jh)_e})_\gamma, \quad \text{and} \quad (A_{(i, j)_e})_{\gamma'} = (A_{(ih, jh)_e})_\gamma. \]

Here, for \((\gamma, e) = 1, \sigma_\gamma \) is the automorphism \( \zeta \mapsto \zeta^h \) of \( \mathbb{Q}(\zeta) \) over \( \mathbb{Q} \).

The cyclotomic problem, i.e., the problem of determining all cyclotomic numbers for a given modulus and a given field, has been considered by various mathematicians since the time of Gauss (1801). The cyclotomic problem for prime modulus \( l \), over finite fields \( F_q^l \), \( q = p^a, p \equiv 1 \) (mod \( l \)), has been treated by Gauss \((l = 2, 3, q = p)\), Stieltjes \((l = 3, q = p)\), Dickson, Whiteman, and Williams \((l = 3, 5, q = p)\), Leonard and Williams \((l = 7, 11, q = p)\), Hall and Storer \((l = 3, q = p^a)\), Parnami, Agrawal, and Rajwade \((l \leq 19, q = p^a)\), and Katre and Rajwade (any \( l, q = p^a)\). For the historical background and references, see [5].

For odd primes \( l \) and modulus \( e = 2l \), the cyclotomic problem for finite fields \( F_q^*, q = p^a, p \equiv 1 \) (mod \( 2l \)) has been treated by Dickson \((e = 6, q = p)\) in detail; \( e = 10, 14, q = p \) sketchy, Whiteman \((e = 10, q = p)\), Muskat \((e = 14, q = p)\), Buck and Williams \((e = 14, q = p)\), Zee \((e = 22, q = p)\),
Berndt and Evans \( (e = 6, q = p^2), \) Hall and Storer \( (e = 6, q = p^4), \) and Acharya and Katre \( (e = 2l, \text{any } l, q = p^2), \) For the references, see [1].

It has been observed by all these authors, and was earlier remarked by Gauss, that for an odd prime \( l \) and \( p \equiv 1 \pmod{l}, \) the cyclotomic numbers of order \( l \) and order \( 2l \) over the field \( \mathbb{F}_q \) cannot be determined just in terms of \( p \) and \( l \) but that one requires, in addition, a quadratic partition of \( q. \) Then the formulae for cyclotomic numbers can be written in terms of a properly chosen solution of a relevant diophantine system; e.g., Gauss obtained cyclotomic numbers of order \( 3 \) in terms of a solution \( (L, M) \) of the system \( 4p = L^2 + 27M^2, \) \( L \equiv 1 \pmod{3}. \) While Gauss used his theory of cyclotomic periods to obtain this diophantine system, Dickson and later authors have used the properties of Jacobi sums for this purpose.

The order of \( p \) modulo \( l, \) written \( \text{ord}_p(l) \), is defined to be the least positive integer \( f \) such that \( p^f \equiv 1 \pmod{l}. \) In other words, earlier authors have considered the case when \( \text{ord}_p(l) = 1 \) in the above works. For \( l = 3, q = p^2, \) Hall and Storer have, in addition, considered the case when \( p \not\equiv 1 \pmod{3} \) (or \( \text{ord}_p(3) = 2). \) When \( \text{ord}_p(l) \) is maximum possible, i.e., \( l - 1, \) Katre and Anuradha [7] have shown that for finite fields \( \mathbb{F}_q, q = p^s \equiv 1 \pmod{l}, \) the cyclotomic numbers and Jacobi sums of order \( l \) can be obtained just in terms of \( q \) and \( l. \)

One of the aims of the present paper is to prove that for \( e = l \) and \( e = 2l, \) and in all cases when \( \text{ord}_p(l) \) is even, the cyclotomic numbers and Jacobi sums of order \( e \) for finite fields \( \mathbb{F}_q, q = p^s \equiv 1 \pmod{e}, \) are given solely and explicitly in terms of \( q \) and \( l \) and one does not have to consider solutions of a specific diophantine system. V. V. Acharya has recently drawn our attention to a paper by Baumert et al. [2] where they have introduced the concept of uniform cyclotomy. Further, the referee has informed us of a paper by R. J. Evans [3] in which the author has explicitly evaluated certain pure Gauss sums over finite fields using results for Jacobi sums. We find that there is some overlapping between the results in these two papers and the results obtained here; however, the methods are different, and we have a number of new results, especially related to \( \zeta \)-functions.

The cyclotomic problem in the case when \( \text{ord}_p(l) \) is odd and \( >1 \) is more intricate and will be treated separately.

In the present paper, we first evaluate the Jacobi sums of order \( e = l \) and \( e = 2l, \) for odd primes \( l, \) over finite fields \( \mathbb{F}_q, q = p^s \equiv 1 \pmod{e}, \) when \( f = \text{ord}_p(2l) \) is even. It has been possible to consider these two cases \( (e = l \text{ and } e = 2l) \) simultaneously, and the Jacobi sums of order \( e \) in each case are elements of the ring \( \mathbb{Z}[[\zeta]], \) In fact, here, the \( J_e(i, j) \) happen to be rational integers: \( -1, q - 2, \) or \( \pm p^2. \) (As \( f \) is even, so is \( \pi. \))

In Theorem 1, we determine the prime ideal decomposition of the Jacobi sums of order \( l \) and order \( 2l \) over \( \mathbb{F}_q \) in the ring \( \mathbb{Z}[[\zeta]], \) this turns out to
be very simple, given solely in terms of the ideal \( p \) of the above ring. We obtain this decomposition using splitting properties of the prime \( p \) in the cyclotomic field \( \mathbb{Q}(\zeta_l) \) and simple properties of the Galois group of \( \mathbb{Q}(\zeta_l) \) over \( \mathbb{Q} \), and interpreting these in the light of some (general) established properties of Jacobi sums. In Theorem 2, we apply a simple lemma related to the cyclotomic ring of integers \( \mathbb{Z}[\zeta_l] \) to determine the Jacobi sums of order \( l \) and order \( 2l \) explicitly in terms of \( q \) (or \( p \)) alone. In Theorem 3, we show that the Jacobi sums obtained directly as above can alternatively be determined in terms of the (unique) solution of a relevant diophantine system; this demonstrates the relationship (for the case considered here) with the work done by earlier authors when \( \text{ord } p \equiv 1 \mod l \).

In Section 4, we see that certain lemmas which determine the cyclotomic numbers in terms of coefficients of the Jacobi sums for the case \( p \equiv 1 \mod e \) \( (e = l, 2l) \) also extend to the case when \( p \) is not necessarily \( \equiv 1 \mod e \). Using the results obtained for Jacobi sums in Theorem 2, we apply these lemmas to obtain explicitly the cyclotomic numbers of order \( l \) and order \( 2l \) for the case under consideration (cf. Theorems 4 and 5).

The results we have obtained for the Jacobi sums and cyclotomic numbers as above are independent of the generator \( \gamma \) of \( \mathbb{F}_q^* \) as well as the root of unity \( \zeta \). In other words, a certain ambiguity that arises in the evaluation of these sums and numbers with respect to the generator \( \gamma \), for the case \( \text{ord } p \equiv 1 \mod l \), does not arise here. Further, the results obtained here are expressed solely in terms of \( q \) and \( l \) (see also \([2, 3]\)).

In Section 5, we illustrate our results through concrete numerical examples. Further, for the case \( l = 3, e = 3, 6 \), we illustrate the compatibility of our results (for \( \text{ord } p \equiv 1 \mod e \) even) with those obtained by earlier authors when \( p \equiv 1 \mod l \). In Section 6, we apply these results to obtain the exact number of points on the non-singular projective curves \( aY^l = bX^l + cZ^l \) and \( aY^{2l} = bX^{2l} + cZ^{2l} \) \( (abc \neq 0) \) defined over the finite field \( \mathbb{F}_q \), \( q = p^e \equiv 1 \mod e \), where \( e = l \) in the first case and \( e = 2l \) in the second case, for odd primes \( l \) and any prime \( p \) such that \( \text{ord } p \equiv 1 \mod l \) is even. These results, obtained in Theorems 6 and 7, are given just in terms of \( q \) and \( l \).

We next apply the results of Theorem 6 to explicitly obtain the \( \zeta \)-function of the projective curve \( aY^l = bX^l + cZ^l \) defined over \( \mathbb{F}_q \) as a rational function in the variable \( t \) (cf. Theorem 8). Thus we are able to corroborate the Weil conjectures (that have been proved in generality) for this concrete class of curves. It is important to mention here that although the \( \zeta \)-function of a non-singular projective curve over a finite field is known to be a rational function in the variable \( t \), of the form \( P(t)/(1-t)(1-qt) \), in general it has been quite difficult to explicitly obtain the polynomial \( P(t) \); this is known in the literature only for a few simple curves.

In conclusion, we remark that the results of this paper may be further applied to determine explicitly the \( \zeta \)-functions of the projective curves...
\[ aY^2 = bX^2 + cZ^2, \quad aY^2Z^{l-2} = bX^2 + cZ^2, \quad \text{and} \quad aY^2Z^{l-2} = bX^2 + cZ^{2l} \]

(\(abc \neq 0\)), defined over certain finite fields, as rational functions in the variable \(t\).

2. PROPERTIES OF JACOBI SUMS AND CYCLOTOMIC NUMBERS

Henceforth in this paper, \(l\) will always denote an odd prime. Further, we will denote, for the finite field \(F_q\), the Jacobi sums and cyclotomic numbers of order \(l\) by \(J_l(i, j)\) and \(A_l(i, j)\), respectively, and those of order \(2l\) by simply \(J(i, j)\) and \(A(i, j)\). These will be defined with respect to the characters on \(F_q^*\),

\[
\chi: \gamma \mapsto \zeta
\]

(for the modulus \(l\)-case), and

\[
\psi: \gamma \mapsto \xi
\]

(for the modulus \(2l\)-case), where \(\gamma\) is a fixed generator of the cyclic group \(F_q^*\) and \(\zeta\) and \(\xi\) are primitive (complex) \(l\)th and \(2l\)th roots of unity, respectively. Further, we will assume that \(\xi = \zeta^2\) (equivalently, \(\zeta = -\xi^{(l+1)/2}\)); this assumption is required when we wish to consider Jacobi sums of order \(l\) and order \(2l\) simultaneously; e.g., this is needed in the proofs of Properties 5 and 8 of Jacobi sums of order \(2l\) given in Proposition 2 below.

2.1. The Case for Modulus \(l\)

For the case \(p \equiv 1 \pmod{l}\), \(q = p^s \equiv 1 \pmod{l}\), the following properties of \(J_l(i, j)\) and \(A_l(i, j)\), for \(i, j\) modulo \(l\), have been established in [9]. Most of these properties have also been observed for the case \(p \not\equiv 1 \pmod{l}\), \(q = p^s \equiv 1 \pmod{l}\), in [7]. The remaining properties are observed easily. The case \(p = 2\) is also included here. We write \(q - 1 = lt\) and state these combined results below as:

Proposition 1. For any prime \(p\) such that \(q = p^s \equiv 1 \pmod{l}\), the following properties are satisfied by the Jacobi sums and cyclotomic numbers of order \(l\) for the finite field \(F_q^*\):

Properties of \(J_l(i, j)\):

1. \(J_l(i, j) = J_l(j, i) = J_l(-i - j, j) = J_l(j, -i - j) = J_l(-i - j, i) = J_l(i, -i - j)\).
2. \[ J_l(0, j) = \begin{cases} -1 & \text{if } j \not\equiv 0 \pmod{l}, \\ q - 2 & \text{if } j \equiv 0 \pmod{l}. \end{cases} \]

3. If \( a + b + c \equiv 0 \pmod{l} \), \( J_l(a, b) = J_l(b, c) = J_l(c, a) \). In particular, \( J_l(1, l - 1) = J_l(1, 0) \).

4. For \((k, l) = 1\), \( \sigma_k J_l(i, j) = J_l(ik, jk) \).

5. \[ J_l(1, n) \frac{J_l(1, n)}{J_l(1, 1)} = \begin{cases} q & \text{if } n \not\equiv 0, -1 \pmod{l}, \\ 1 & \text{if } n \equiv 0, -1 \pmod{l}. \end{cases} \]

6. \( J_l(1, n) \equiv -1 \pmod{(1 - \zeta)^2} \).

Remark. From Properties 1-4 above, we see that to obtain all Jacobi sums of order \( l \), it is enough to determine \( J_l(1, 1), J_l(1, 2), \ldots, J_l(1, (l - 1)/2) \) when \( l > 3 \) and \( J_l(1, 1) \) when \( l = 3 \). (Note that \( J_l(1, (l - 1)/2) = J_l((l - 1)/2, (l - 1)/2) = \sigma_{l - 1/2} J_l(1, 1) \).

Properties of \( A_{(i, j)} \):

1. \[ A_{(i, j)} = A_{(j, i)} = A_{(i + j, l - i - j)} = A_{(l - i - j, j)} = A_{(l - i, j - i)} = A_{(l - j, i - j)}, \]

2. \[ \sum_{j=0}^{l-1} A_{(i, j)} = \{ \begin{array}{ll} t - 1 & \text{if } i \equiv 0 \pmod{l}, \\ t & \text{if } i \not\equiv 0 \pmod{l}. \end{array} \]

3. \[ \sum_{i=0}^{l-1} \sum_{j=0}^{l-1} A_{(i, j)} = q - 2. \]

2.2. The Case for Modulus \( 2l \)

For the case \( p \equiv 1 \pmod{2l} \), \( q = p^* \equiv 1 \pmod{2l} \), the following properties of \( J(i, j) \) and \( A_{i, j} \), for \( i, j \) modulo \( 2l \), have been established in [1]. We observe that these properties also hold for the case \( p \not\equiv 1 \pmod{2l} \), \( q = p^* \equiv 1 \pmod{2l} \). The proofs are analogous to the case established in [1]. The case \( p = 2 \) does not arise here. We write \( q - 1 = 2lt \) and combine these results to give:

**Proposition 2.** For any odd prime \( p \) such that \( q = p^* \equiv 1 \pmod{2l} \), the following properties are satisfied by the Jacobi sums and cyclotomic numbers of order \( 2l \) for the finite field \( \mathbb{F}_q \):

Properties of \( J(i, j) \):

1. \[ J(i, j) = \psi^{l*}(1) J(i, j) = (1 - i - j) J(i, j) = \psi^l(1) J(i, j) = \psi^{l*}(1) J(i, j) = \psi^l(1) J(i, j). \]
2. If \( a + b + c \equiv 0 \pmod{2l} \), then \( J(a, b) = \psi'(-1) J(b, a) = J(c, b) = \psi''(-1) J(b, c) = \psi''(-1) J(c, a) = \psi''(-1) J(a, c) \). In particular, \( J(1, n) = \psi(-1) J(1, 2l - n - 1) \).

3. \( J(0, j) = \begin{cases} -1 & \text{if } j \not\equiv 0 \pmod{2l}, \\ q - 2 & \text{if } j \equiv 0 \pmod{2l}. \end{cases} \)

\( J(i, 0) = \psi'(-1) J(0, i) \).

4. For \( (k, 2l) = 1 \), \( \tau_k J(i, j) = J(ik, jk) \), where \( \tau_k \) is the automorphism \( \zeta \mapsto \zeta^k \) of \( \mathbb{Q}(\xi) \) over \( \mathbb{Q} \) (this is equivalent to the automorphism \( \sigma_k : \zeta \mapsto \zeta^k \) of \( \mathbb{Q}(\zeta) \) over \( \mathbb{Q} \)).

5. \( J(2r, 2s) = J(r, s) \).

6. \( J(1, n) J(1, n) = \begin{cases} q & \text{if } n \not\equiv 0 \pmod{2l}, \\ 1 & \text{if } n \equiv 0 \pmod{2l}, \end{cases} \)

7. Let \( m, n, r \) be integers such that \( m + n \not\equiv 0 \pmod{2l} \) and \( m + r \not\equiv 0 \pmod{2l} \). Then \( J(m, n) J(m + n, r) = \psi''(-1) J(m, r) J(n, m + r) \).

8. Let \( n \) be an odd integer such that \( 1 \leq n \leq 2l - 3 \) and let \( m = \text{ind} \). Then \( J(1, n) \equiv -\zeta^{-m(n+1)} \pmod{(1 - \zeta)^2} \). If \( n \) is even such that \( 2 \leq n \leq 2l - 2 \), then \( J(1, n) = \psi(-1) J(1, 2l - n - 1) \equiv -\psi(-1) \zeta^{mn} \pmod{(1 - \zeta)^2} \).

Properties of \( A_{i, j} \):

1. For \( t \) even, \( A_{i, j} = A_{i, j} = A_{i - k, j - k} = A_{i - j, i - j} = A_{i - k, j - i} = A_{i - j, i - j} \).

For \( t \) odd, \( A_{i, j} = A_{i + k, j + k} = A_{i + k, i - j} = A_{i + j, i - k} = A_{i + j, i - i} = A_{i + j, i - j} \).

\[ \sum_{j=0}^{2l-1} A_{i, j} = t - n_i, \] where

\[ n_i = \begin{cases} 1 & \text{if } i \equiv 0 \pmod{2l}, t \text{ even}, \\ 1 & \text{if } i \equiv l \pmod{2l}, t \text{ odd}, \\ 0 & \text{otherwise}. \end{cases} \]

\[ \sum_{i=0}^{2l-1} A_{i, j} = \begin{cases} t - 1 & \text{if } j \equiv 0 \pmod{2l}, \\ t & \text{if } j \not\equiv 0 \pmod{2l}. \end{cases} \]

3. \( \sum_{i=0}^{2l-1} \sum_{j=0}^{2l-1} A_{i, j} = q - 2. \)

Remark. From the properties of \( J(i, j) \), it follows that we may obtain all the \( 4l^2 \) Jacobi sums of order \( 2l \) if
(i) we know all the Jacobi sums of order \( l \) and

(ii) we know the Jacobi sums \( J(1, n) \) for \( n \) odd, \( 1 \leq n \leq 2l - 3 \) (equivalently, if we know \( J(1, n) \) for \( n \) even, \( 2 \leq n \leq 2l - 2 \)).

Thus, to obtain all \( J(i, j) \), it is enough to determine \( J(1, n) \) for \( n \) odd, \( 1 \leq n \leq 2l - 3 \), and \( J(1, n) \) for \( 1 \leq n \leq (l - 3)/2 \) when \( l > 3 \). For \( l = 3 \), we need to know \( J(1, 1) \), \( J(1, 1) \), and \( J(1, 3) \).

2.3. The Subcase When \( \text{ord}_p(p \mod l) \) is Even, for Moduli \( e = l \) and \( e = 2l \)

Let the order \( \text{ord}_p(p \mod l) \) be even. For \( e = l, 2l \) and \( q = p^s \equiv 1 \mod e \), one sees that \( x = fs \) for some integer \( s \geq 1 \). Thus \( q - 1 \equiv 0 \mod 4 \) when \( p \neq 2 \). So for modulus \( e = 2l \), and \( q - 1 = 2lt \), it follows that \( t \) is even and \( \psi(-1) = 1 \).

Also, for this subcase, we see that when \( p \neq 2 \), ind, \( 2 \equiv 0 \mod l \) in the finite field \( F_q \). (In fact, each element of \( F_q \) is an \( l \)th power in \( F_q \).) This follows by noting that

\[ F_p = \{ 0, \gamma^j, \gamma^{2j}, \ldots, \gamma^{(p-1)j} \} \subseteq F_q, \]

where \( j = (q - 1)/(p - 1) \); clearly \( j \equiv 0 \mod l \). Thus we may combine the results of Propositions 1 and 2 to obtain:

**Proposition 3.** For \( e = l \) and \( e = 2l \), when \( \text{ord}_p(p \mod l) \) is even and \( q = p^s \equiv 1 \mod e \), setting \( q - 1 = et \), the Jacobi sums and cyclotomic numbers of order \( e \) for the finite field \( F_q \) satisfy the following properties:

**Properties of \( J_e(i, j) \):**

1. \( J_e(i, j) = J_e(j, i) = J_e(-i - j, j) = J_e(-i - j, i) = J_e(i, -i - j) \).

2. \( J_e(0, j) = \begin{cases} -1 & \text{if } j \not\equiv 0 \mod e, \\ q - 2 & \text{if } j \equiv 0 \mod e. \end{cases} \)

3. If \( a + b + c \equiv 0 \mod e \), \( J_e(a, b) = J_e(b, c) = J_e(c, a) \). In particular, \( J_e(1, n) = J_e(1, e - n - 1) \) and \( J_e(1, e - 1) = J_e(1, 0) \).

4. If \( a + b \equiv 0 \mod e \) and \( a, b \neq 0 \mod e \), then \( J_e(a, b) = -1 \).

5. For \( (k, e) = 1 \), \( \sigma_k J_e(i, j) = J_e(ik, jk) \).

6. \( J_e(1, n) J_e(1, n) = \begin{cases} q & \text{if } n \not\equiv 0 \mod e, -1, \\ 1 & \text{if } n \equiv 0 \mod e. \end{cases} \)
7. \(J_{\ell}(1, n) = -1 \pmod{1 - \zeta^2}\).

8. For \(e = 2l\), \(J_{\ell}(2l, 2e) = J_{\ell}^{2}(r, s)\) and \(J_{\ell}(m, n)\) \(J_{\ell}(m + n, r) = J_{\ell}(m, r)\) \(J_{\ell}(n, m + r)\) for \(m + n, m + r \not\equiv 0 \pmod{e}\).

Properties of \(A(i, _{\ell})\):

1. \(A_{i, P(1, 2)} = A_{i, P(1, 2)} = A_{i, P(1, 2)} = A_{i, P(1, 2)} = A_{i, P(1, 2)} = A_{i, P(1, 2)}\).

2. \(\sum_{i=0}^{e-1} \sum_{j=0}^{e-1} A_{i, j} = q - 2.\)

3. \(\sum_{i=0}^{e-1} \sum_{j=0}^{e-1} A_{i, j} = q - 2.\)

3. EVALUATION OF JACOBI SUMS OF ORDER \(l, 2l\)

**Theorem 1** (Prime Ideal Decomposition of the Jacobi Sums). Let \(p\) be a prime such that \(f = \text{ord} p \pmod{e}\) is even, and let \(q = p^e \equiv 1 \pmod{e}\) where \(e = l\) or \(2l\). Then for the finite field \(F_q\), the prime ideal decomposition of \(J_{\ell}(1, n)\) in \(\mathbb{Z}[\zeta]\) is given by \((J_{\ell}(1, n)) = (p^{n/2})\) for \(1 \leq n \leq e - 2\).

**Proof.** First, we note that all the Jacobi sums of order \(l\) and order \(2l\) belong to the ring \(\mathbb{Z}[\zeta]\) (as the cyclotomic fields \(\mathbb{Q}(\zeta)\) and \(\mathbb{Q}(\xi)\) are the same). Second, we have

\[\overline{J_{\ell}(1, n)} = \overline{J_{\ell}(1, n)} = q \quad \text{for} \quad 1 \leq n \leq e - 2\]

(cf. Proposition 3). Thus any prime factor occurring in the prime ideal decomposition of \((J_{\ell}(1, n))\) in \(\mathbb{Z}[\zeta]\) is necessarily some prime factor of the ideal \((p)\), and of no ideal coprime to \((p)\), in \(\mathbb{Z}[\zeta]\).

Let \(G = \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{\sigma_1, \sigma_2, ..., \sigma_{l-1}\}\), where \(\sigma_i\) is the automorphism \(\zeta \mapsto \zeta^i\) of \(\mathbb{Q}(\zeta)\) over \(\mathbb{Q}\) for each \(i = 1, ..., l - 1\).

We know from algebraic number theory that

\[(p) = \mathcal{P}_1 \mathcal{P}_2 \cdots \mathcal{P}_k \subset \mathbb{Z}[\zeta]\]

where \(k = (l - 1)/f\) and \(\mathcal{P}_i\)'s, \(i = 1, ..., k\), are distinct primes in \(\mathbb{Z}[\zeta]\). We also know that the decomposition group \(G_{\mathcal{P}} = \{\sigma \in G \mid \sigma(\mathcal{P}) = \mathcal{P}\}\) is the same for each \(\mathcal{P} = \mathcal{P}_i\), \(1 \leq i \leq k\), and that \(G_{\mathcal{P}}\) is a subgroup of \(G\) of order \(f\). This subgroup is unique as \(G\) is cyclic. Since \(f\) is even, there is an element of order \(2\) in \(G_{\mathcal{P}}\). Clearly, this is the (unique) automorphism \(\sigma_{-1} : \zeta \mapsto \zeta^{-1}\) of \(\mathbb{Q}(\zeta)\) over \(\mathbb{Q}\). Thus \(\sigma_{-1}(\mathcal{P}) = \mathcal{P}\) for each \(\mathcal{P} = \mathcal{P}_i\), \(1 \leq i \leq k\). Noting that \(J_{\ell}(1, n) = \sigma_{-1}J_{\ell}(1, n)\), we obtain:

\[(J_{\ell}(1, n)) = (\overline{J_{\ell}(1, n)}) \subset \mathbb{Z}[\zeta].\]
Since $J_e(1, n) J_e(1, n) = q = p^s$ for $1 \leq n \leq e - 2$, it follows that

$$J_e(1, n) = (p^{\pi/2}) \in \mathbb{Z}[\zeta] \quad \text{for} \quad 1 \leq n \leq e - 2.$$ 

Note that $\pi$ is even, since $\pi = fs$ for some integer $s \geq 1$.

**Lemma 1.** Let $\alpha, \beta \in \mathbb{Z}[\zeta]$, both prime to $1 - \zeta$, satisfy:

(i) $(\alpha) = (\beta)$,

(ii) $|\alpha| = |\beta|$, and

(iii) $\alpha \equiv \beta \pmod{(1 - \zeta)^2}$.

Then $\pi = \beta$.

**Proof.** See, for example, [9, Lemma 5, §2].

**Theorem 2.** Let $p$ be any prime such that $f = \text{ord}_p \pmod{l}$ is even, and let $q = p^s \equiv 1 \pmod{e}$, for $e = l$ or $2l$. Then $\pi = fs$ for some integer $s \geq 1$ and the Jacobi sums of order $e$ for the finite field $\mathbb{F}_q$ are given explicitly as:

$$J_e(1, n) = (-1)^{s-1} q^{1/2} \quad \text{for} \quad 1 \leq n \leq e - 2.$$ 

**Proof.** Since $f = \text{ord}_p \pmod{l}$, and $f$ is even, it follows that $p^{\pi/2} \equiv -1 \pmod{l}$. Thus $p^{\pi/2} \equiv (-1)^{l/2} \pmod{l}$. This implies that $p^{\pi/2} \equiv (-1)^l \pmod{l - \zeta^2}$ in $\mathbb{Z}[\zeta]$. Thus, for $1 \leq n \leq e - 2$, the elements $J_e(1, n)$ and $(-1)^{s-1} p^{\pi/2}$ of $\mathbb{Z}[\zeta]$ have the same prime ideal decomposition, the same absolute value, and the same congruence relation modulo $(1 - \zeta^2)$ (cf. Theorem 1 and Proposition 3). By Lemma 1, the theorem follows.

**Remark.** Thus, when $\text{ord}_p \pmod{l}$ is even, it is clear that the Jacobi sums of order $l$ and order $2l$ for the finite field $\mathbb{F}_q$ are independent of the generator $\gamma$ of $\mathbb{F}_q^*$ and the root of unity $\zeta$.

Alternatively, for the case under consideration, the Jacobi sums of order $l$ and order $2l$ are determined in terms of the (unique) solution of the diophantine system in Theorem 3 below:

**Theorem 3.** For any prime $p$ such that $f = \text{ord}_p \pmod{l}$ is even, let $q = p^s \equiv 1 \pmod{e}$, for $e = l$ or $2l$. Then $\pi = fs$ for some integer $s \geq 1$. Let $H = \sum_{i \pmod{l}} a_i \zeta^i \in \mathbb{Z}[\zeta]$ (where we may (or may not) give any fixed value to one of the $a_i$). Suppose the $a_i$ satisfy the arithmetic conditions (or the diophantine system):

(i) $q = \sum_{i=0}^{l-1} \frac{a_i}{i} - \sum_{i=0}^{l-1} a_i a_{i+1}$.
\[
\sum_{i=0}^{l-1} a_i a_{i+1} = \sum_{i=0}^{l-1} a_i a_{i+2} = \cdots = \sum_{i=0}^{l-1} a_i a_i = 0,
\]

(iii) \(1 + a_0 + \cdots + a_{l-1} \equiv 0 \pmod{l},\)

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

(v) \(a_i = a_{i-1} \pmod{l},\)

then \(H = J_e(1, n)\) for \(1 \leq n \leq e-2\), where \(J_e(1, n)\) is defined with respect to any generator of \(\mathbb{F}_{q^*}\), and the converse. The above system has the unique solution \(H = (-1)^{r-1} p^{n/2}\). (The \(a_i's\) are obtained uniquely by giving a fixed value to any one of them.)

**Proof.** The arithmetic conditions (i) and (ii) are equivalent to the condition \(HH = q\), and conditions (iii) and (iv) are equivalent to the condition \(H \equiv -1 \pmod{1-\zeta^2}\). (See, for example, [9, §3].) Condition (v) is equivalent to the condition \(H = H\). The conditions \(HH = q\) and \(H = H\) together give the ideal decomposition of \(H\) in \(\mathbb{Z}[\zeta]\) as \((H) = (p^{n/2})\). By Lemma 1, \(H\) is uniquely determined as an element of \(\mathbb{Z}[\zeta]\). The above conditions on \(H\), viz. the absolute value, the prime ideal decomposition, and the congruence relation modulo \((1-\zeta)^2\), are also satisfied by the Jacobi sums \(J_e(1, n)\) for \(1 \leq n \leq e-2\) (cf. Theorem 1 and Proposition 3) and by the element \((-1)^{r-1} p^{n/2}\) of \(\mathbb{Z}[\zeta]\). By Lemma 1, the theorem follows.

**Remark.** Theorem 3 relates the evaluation of Jacobi sums as determined in Theorem 2 to the work done by earlier authors when \(\text{ord } p \equiv 1 \pmod{l}\) (see [5, 1] and the references therein).

### 4. EVALUATION OF CYCLOTOMIC NUMBERS

#### 4.1. Cyclotomic Numbers of Order \(l\)

For a finite field \(\mathbb{F}_q\), \(q \equiv 1 \pmod{l}\), the Dickson–Hurwitz sums of order \(l\) over \(\mathbb{F}_q\) have been defined, for \(j, n\) modulo \(l\), by

\[
B_l(j, n) = \sum_{i=0}^{l-1} A(i, j-ni),
\]

For the case \(p \equiv 1 \pmod{l}\), \(q = p^e \equiv 1 \pmod{l}\), the cyclotomic numbers and the Dickson–Hurwitz sums of order \(l\) over \(\mathbb{F}_q\) have been determined in terms of the coefficients of certain Jacobi sums of order \(l\) (see [5, Lemma 5]). We observe that these formulae also hold true for all other cases of \(\text{ord } p \equiv 1 \pmod{l}\); the proofs are analogous to the case \(p \equiv 1 \pmod{l}\) considered in [5]. We combine these results to give:
Lemma 2. Let $p$ be any prime and let $q = p^s \equiv 1 \pmod{l}$. Let $J_l(1, n) = \sum_{i=1}^{l-1} a_i(n) \xi^i$ be the Jacobi sums of order $l$ over $\mathbb{F}_q$, for $n \equiv l-1 \pmod{l}$. Then the corresponding Dickson–Hurwitz sums and the cyclotomic numbers of order $l$ over $\mathbb{F}_q$ are given by

$$lB_l(j, n) = la_j(n) + (q - 2) - \sum_{i=1}^{l-1} a_i(n),$$

and

$$l^2 A_{(i, j)} = q - 3l + 1 + \varepsilon(i) + \varepsilon(j) + \varepsilon(i - j) + l \sum_{n=1}^{l-2} a_{m+j}(n) - \sum_{n=1}^{l-2} \sum_{k=1}^{l-1} a_k(n),$$

where

$$a_0(n) = 0, \quad \varepsilon(i) = \begin{cases} 0 & \text{if } l \nmid i, \\ 1 & \text{if } l \mid i, \end{cases}$$

and the suffixes in $a_{m+j}(n)$ are considered modulo $l$.

In particular,

$$l^2 A_{(0, 0)} = q - 3l + 1 - \sum_{n=1}^{l-2} \sum_{k=1}^{l-1} a_k(n),$$

and

$$l^2 A_{(i, j)} = \varepsilon(i) + \varepsilon(j) + \varepsilon(i - j) + l \sum_{n=1}^{l-2} a_{m+j}(n) + l^2 A_{(0, 0)}. $$

We now explicitly obtain the cyclotomic numbers of order $l$ for the case under consideration in this paper.

Theorem 4. For any prime $p$ such that $f = \text{ord } p \pmod{l}$ is even, for $q = p^s \equiv 1 \pmod{l}$, and $x = fs$, for $s \geq 1$, the cyclotomic numbers of order $l$ over $\mathbb{F}_q$ are given by:

$$l^2 A_{(0, 0)} = q - 3l + 1 - (l-1)(l-2)(-1)^s q^{1/2},$$

$$l^2 A_{(0, j)} = q - l + 1 + (l-2)(-1)^s q^{1/2} \quad \text{for } j \equiv 0 \pmod{l},$$

$$l^2 A_{(i, j)} = q + 1 - 2(-1)^s q^{1/2} \quad \text{for } i, j, i-j \not\equiv 0 \pmod{l}.$$

Note that $A_{(0, 0)} = A_{(i, j)} = A_{(-i, -j)}$. 

299 NUMBER OF POINTS ON PROJECTIVE CURVES
Proof. From Theorem 2,
\[ J_l(1, n) = (-1)^{r-1} p^{x^2} \sum_{i=1}^{l-1} (-1)^i p^{x^2 \xi_i}, \quad \text{for} \quad 1 \leq n \leq l-2. \]
So if we write \( J_l(1, n) = \sum_{i=1}^{l-1} a_i(n) \xi_i \), it follows that
\[ a_i(n) = (-1)^i p^{x^2} = (-1)^i q^{1/2} \quad \text{for each} \quad 1 \leq i \leq l-1, \quad 1 \leq n \leq l-2. \]
The theorem now follows from Lemma 2.

4.2. Cyclotomic Numbers of Order 2l

For the case \( p \equiv 1 \pmod{2l} \), \( q = p^s \), the cyclotomic numbers of order 2l for the finite field \( \mathbb{F}_q \) have been determined in terms of the coefficients of certain Jacobi sums of order \( l \) and order 2l (see [1, Proposition 7]). We observe that the same relations hold true for the case \( p \not\equiv 1 \pmod{2l} \), \( q = p^s \equiv 1 \pmod{2l} \). This is seen by noting the following:

For the proof in [1, Proposition 7], the Dickson–Hurwitz sums of order 2l have been considered and the Jacobi differences \( D(j, n) \) have been defined in terms of these. Further, following Whiteman [12], the numbers \( s(i, j) \) and \( t(i, j) \) have been defined in terms of cyclotomic numbers of order 2l. The Dickson–Hurwitz sums of order 2l, \( B_{2l}(j, n) = B(j, n) \), are defined for \( j, n \) modulo 2l by
\[ B(j, n) = \sum_{i=0}^{2l-1} A_{k, j - m}. \]
The Jacobi differences \( D(j, n) \) have been defined as
\[ D(j, n) = B(j, n) - B(j + l, n), \]
and the numbers \( s(i, j) \) and \( t(i, j) \) have been defined as
\[ s(i, j) = A_{k, j} - A_{k, j + l} \quad \text{and} \quad t(i, j) = A_{k, j} - A_{k + l, j}. \]
The above terms and numbers are defined solely in terms of cyclotomic numbers of order 2l. It follows that certain properties and relations satisfied by these terms and numbers, seen in [1] for the case \( \text{ord } p \pmod{l} = 1 \), also carry over to all other cases of \( \text{ord } p \pmod{l} \). This follows from the properties of \( A_{k, j} \) as seen in Proposition 2.

Relations have been obtained in [1, Section 5] that express \( s(i, j) \) and \( t(i, j) \) in terms of the Jacobi differences \( D(j, n) \). Further, relations have also been obtained in [1, Section 5] that determine the Dickson–Hurwitz sums.
and the Jacobi differences in terms of the coefficients of Jacobi sums of order \( l \) and order \( 2l \). Noting that the properties of \( J_l(i, j) \) and \( J(2l) \) are respectively the same for all cases of \( p \equiv \pm 1 \pmod{2l} \) (cf. Propositions 1, 2), we can see that these relations continue to hold true for the case \( p \equiv 1 \pmod{2l} \). The proofs and the reasoning are the same as in [1]. For the statements of these relations, see [1, Propositions 5, 5, and 6 and Corollaries 1, 2].

In [1, Proposition 7], for the case \( p \equiv 1 \pmod{2l} \), the cyclotomic numbers of order \( 2l \) have been determined in terms of the coefficients of Jacobi sums of order \( l \) and order \( 2l \) by applying the above-mentioned relations and a certain lemma [5, Lemma 5]. By our observations in the preceding paragraph, and noting that Lemma 5 in [5] extends to all cases of \( p \equiv \pm 1 \pmod{2l} \) (cf. Lemma 2), it is not difficult to verify that the relations in [1, Proposition 7] extend to the case \( p \equiv 1 \pmod{2l} \), \( q = p^s \equiv 1 \pmod{2l} \). The proof and the reasoning are the same. We combine these results below as:

**Lemma 3.** For any odd prime \( p \) such that \( q = p^s \equiv 1 \pmod{2l} \), let

\[
J_l(1, n) = \sum_{i=1}^{l-1} a_i(n) \zeta^i \quad \text{and} \quad J(1, n) = \sum_{i=1}^{l-1} b_i(n) \zeta^i
\]

be the Jacobi sums of order \( l \) and order \( 2l \) over \( \mathbb{F}_q \). Then

\[
A_{l, j} = q - 3l + 1 + \ell(i) + \ell(j) + \ell(i-j) + \ell(2u+1) \sum_{n=0}^{l-2} a_{m+j}(n) - \sum_{n=1}^{l-2} \sum_{k=1}^{l-1} a_k(n)
\]

\[
\times \left\{ l + \sum_{k=1}^{l-1} b_k(l) + \sum_{u=0}^{l-2} \sum_{k=1}^{l-1} b_k(2u+1) \right\}
\]

\[
+ (-1)^{j+l} l \left\{ b_{n-i}(l) + \sum_{u=0}^{l-1} b_{n-i-2u+2j}(2u+1) \right\}
\]

\[
+ (-1)^{i+j} l \left\{ b_{n-j}(l) + \sum_{u=0}^{l-1} b_{n-j+2u+j}(2u+1) \right\}
\]

\[
+ (-1)^{i+j} l \left\{ b_{n-j}(l) + \sum_{u=0}^{l-1} b_{n-i-2u+2j}(2u+1) \right\},
\]

where \( a_0(n) = b_0(n) = 0 \),

\[
v(j) = \begin{cases} 
A(j)/2 & \text{if } j \text{ is even}, \\
A(j+1)/2 & \text{if } j \text{ is odd}, 
\end{cases}
\]
A(r) being defined as the least non-negative residue of r modulo 2l, and

\[ \varepsilon(i) = \begin{cases} 0 & \text{if } l \nmid i, \\ 1 & \text{if } l \mid i. \end{cases} \]

We now explicitly obtain the cyclotomic numbers of order 2l for the case under consideration in this paper.

**Theorem 5.** For any prime p such that \( f = \text{ord } p \pmod{2l} \) is even, for \( q = p^s \equiv 1 \pmod{2l} \), and \( z = fs \), for \( s \geq 1 \), the cyclotomic numbers of order 2l over \( \mathbb{F}_q \) are given by:

\[
\begin{align*}
4l^2A_{0,0} &= q - 6l + 1 - (4l^2 - 6l + 2)(-1)^r q^{1/2}, \\
4l^2A_{0,j} &= q - 2l + 1 + 2(l-1)(-1)^r q^{1/2} \quad \text{for } j \not\equiv 0 \pmod{2l}, \\
4l^2A_{i,j} &= q + 1 - 2(-1)^r q^{1/2} \quad \text{for } i, j, i-j \not\equiv 0 \pmod{2l}.
\end{align*}
\]

Note that \( A_{0,j} = A_{-j,-j} \).

**Proof.** In Theorem 2, we have seen that for \( e = l \) and \( e = 2l \),

\[ J_e(1, n) = (-1)^{e-1} \sum_{i=1}^{l} (-1)^r p^{n/2} \zeta^i, \quad \text{for } 1 \leq n \leq e - 2. \]

So if we write \( J_l(1, n) = \sum_{i=1}^{l-1} a_i(n) \zeta^i \) and \( J_{2l}(1, n) = J(1, n) = \sum_{i=1}^{l-1} b_i(n) \zeta^i \), it follows that

\[ a_i(n) = (-1)^r q^{1/2} \quad \text{for } 1 \leq i \leq l - 1, \quad 1 \leq n \leq l - 2, \]

and

\[ b_i(n) = (-1)^r q^{1/2} \quad \text{for } 1 \leq i \leq l - 1, \quad 1 \leq n \leq 2l - 2. \]

Also, since \( J(1, 0) = J(1, -1) = -1 \), we have

\[ b_i(n) = 1 \quad \text{for } 1 \leq i \leq l - 1, \quad n = 0, 2l - 1. \]

We now apply Lemma 3 to obtain \( A_{i,j} \) for different cases of \( i, j \pmod{2l} \). For this, consider \( 0 \leq i, j \leq 2l - 1 \). Initially, we need to consider the following cases for \( (i, j) \) separately:

(i) \((0, 0)\),
(ii) \((0, j)\) for \( j \not\equiv 0, l \),
(iii) \((0, l)\),
(iv) \((i, l)\) for \( i \not\equiv 0, l \).
The results obtained for these seven cases are then combined to get the results as stated in this theorem.

Remark. It is thus clear that when \( \text{ord } p \pmod{l} \) is even, the cyclotomic numbers of order \( l \) and order \( 2l \) for the finite field \( F_q \) are independent of the generator \( \gamma \) of \( F_q^* \).

5. ILLUSTRATIONS AND EXAMPLES

In this section, we illustrate the results of Theorems 2–5 for the case \( p \equiv 2 \pmod{3} \), \( q = p^s \equiv 1 \pmod{e} \), when \( e = 3 \) and \( e = 6 \). For this case, we obtain explicitly the Jacobi sums of order 3 and order 6 for the field \( F_q \) via the diophantine system of Theorem 3. We then apply Lemmas 2 and 3 to obtain the cyclotomic numbers of order 3 and order 6. We see that these results are in keeping with those obtained directly via Theorems 2, 4, and 5. Further, we observe that these results are compatible with those obtained by earlier authors for the case when \( p \equiv 1 \pmod{3} \). This demonstrates the link between the results we have obtained in Theorems 2, 4, and 5 (for the case when \( p \equiv 1 \pmod{l} \)) and the results obtained by earlier authors in terms of solutions of appropriate diophantine systems (for the case when \( p \equiv 1 \pmod{l} \)).

We then illustrate the results of Theorems 2, 4, and 5 by concrete numerical examples. These results are verified to be in keeping with those obtained by direct calculation via the computer.

**Proposition 4.** Let \( p \) be a prime \( \equiv 2 \pmod{3} \), and let \( q = p^s \equiv 1 \pmod{e} \), where \( e = 3 \) or \( e = 6 \). Thus, \( \text{ord } p \pmod{3} = 2 \) and \( \alpha = 2s \) for some integer \( s \geq 1 \). Note that if \( e = 6 \), the case \( p = 2 \) does not arise. Let \( \omega = e^{2\omega} \).

Then with respect to any generator of \( F_q^* \), the Jacobi sums of order \( e \) for the finite field \( F_q \) are uniquely given by

\[
J_e(1, n) = (L + 3M)/2 + 3M\omega, \quad \text{for } 1 \leq n \leq e - 2,
\]

where

\[
L = 2(-1)^{s-1} q^{1/2} \quad \text{and} \quad M = 0,
\]

and the cyclotomic numbers of order \( e \) for this field are uniquely given, for \( L \) and \( M \) as above, by:
\begin{align*}
A_{(0, 0)} &= (q - 8 + L)/9 = (q - 8 - 2(-1)^r q^{1/2})/9, \\
A_{(0, 1)} &= A_{(1, 0)} = A_{(2, 2)} = (2q - 4 - L + 9M)/18 \\
&= (q - 2 + (-1)^r q^{1/2})/9, \\
A_{(0, 2)} &= A_{(2, 0)} = A_{(1, 1)} = (2q - 4 - L - 9M)/18 \\
&= (q - 2 + (-1)^r q^{1/2})/9, \\
A_{(1, 2)} &= A_{(2, 1)} = (q + 1 + L)/9 = (q + 1 - 2(-1)^r q^{1/2})/9, \\
36A_{0, 0} &= q - 17 + 10L = q - 17 - 20(-1)^r q^{1/2}, \\
36A_{0, 1} &= q - 5 - 2L + 27M = q - 5 + 4(-1)^r q^{1/2}, \\
36A_{0, 2} &= q - 5 - 2L + 9M = q - 5 + 4(-1)^r q^{1/2}, \\
36A_{0, 3} &= q - 5 - 2L - 27M = q - 5 + 4(-1)^r q^{1/2}, \\
36A_{0, 4} &= q - 5 - 2L - 9M = q - 5 + 4(-1)^r q^{1/2}, \\
A_{1, 2} &= A_{1, 3} = A_{1, 4} = A_{2, 4} = (q + 1 + L)/36 = (q + 1 - 2(-1)^r q^{1/2})/36.
\end{align*}

Here, $A_{i, j}$ denote cyclotomic numbers of order 6; the remaining $A_{i, j}$ are given in terms of those listed above by the relations $A_{i, j} = A_{j, i} A_{6-i, 6-j}$. cf. Proposition 3.

**Proof.** Applying Theorem 3, if we fix $a_2 = 0$ and set $H = a_0 + a_1 \omega \in \mathbb{Z}[\omega]$, then Conditions i-v of the theorem reduce to:

\begin{align*}
4q &= (2a_0 - a_1)^2 + 3a_1^2, & a_0 \equiv -1 \pmod{3} \quad \text{and} \quad a_1 = 0.
\end{align*}

If we set $L = 2a_0 - a_1$ and $M = a_1/3$, we obtain:

\begin{align*}
4q &= L^2 + 27M^2, & L \equiv 1 \pmod{3}, & M = 0,
\end{align*}

and

\begin{align*}
J_{d}(1, n) &= H = (L + 3M)/2 + 3M \omega, & 1 \leq n \leq e - 2, & e = 3, 6.
\end{align*}

(See also [9, Proposition 1].) Noting that $q^{1/2} = p^r \equiv (-1)^r \pmod{3}$, it follows that $L = 2(-1)^r q^{1/2}$. Hence, $J_{d}(1, n) = L/2 = (-1)^r q^{1/2}$ for $1 \leq n \leq e - 2$ and $e = 3, 6$. Then, applying Lemmas 2 and 3, the cyclotomic numbers of order 3 and 6 have been obtained as above. These results are in keeping with those obtained alternatively by Theorems 2, 4, and 5. For a comparison with the work done by earlier authors, see [10, 9, 5, 1]. We note that these results for cyclotomic numbers of order 3 are in keeping with those obtained by Storer [10] when $p \equiv 2 \pmod{3}$. Further, these
results for cyclotomic numbers of order 3 and order 6 are compatible with
those obtained by Acharya and Katre [1] for the case $p \equiv 1 \pmod{3}$ when
$m = \text{ind}, 2 \equiv 0 \pmod{3}$. We remark here that while earlier authors have set
$q = ef + 1$ in their works, we have set $q = et + 1$ and $f = \text{ord } p \pmod{l}$.

Remark. Similar results can be obtained for the case $l = 5$, $p \not\equiv 1 \pmod{5}$. In this case, $\text{ord } p \pmod{5}$ is always even. Here too, the results
obtained for Jacobi sums and cyclotomic numbers of order $e = 5$ and $e = 10$
are seen to be compatible with the corresponding results obtained for $p \equiv 1 \pmod{5}$ by earlier authors. The formulae here are more elaborate and will
be treated in a separate paper.

Example 1. Take $p = 19$, $q = p^2 = 361$, $l = 5$. Here, $s = 1$, $f = 2$. By
Theorem 2, with respect to any generator $\gamma$ of $\mathbb{F}_{361}$, the Jacobi sums of
order 5 and 10 for the field $\mathbb{F}_{361}$ are obtained as:

$$J_5(1, n) = 19 \text{ for } 1 \leq n \leq 3 \text{ and } J_{10}(1, n) = 19 \text{ for } 1 \leq n \leq 8.$$

Thus all the Jacobi sums of order $e = 5$ and $e = 10$ for the finite field $\mathbb{F}_{361}$
are determined by Proposition 3 to be:

$$J_5(0, 0) = 359,$$

$$J_5(i, 0) = J_5(0, i) = -1 \text{ for } 1 \leq i \leq e - 1,$$

$$J_5(i, j) = -1 \text{ for } 1 \leq i, j \leq e - 1, \ i + j \equiv 0 \pmod{e},$$

$$J_5(i, j) = 19 \text{ for } 1 \leq i, j \leq e - 1, \ i + j \not\equiv 0 \pmod{e}.$$

The cyclotomic numbers of order 5 and order 10 for the finite field $\mathbb{F}_{361}$ are
determined by Theorems 4 and 5 to be:

$$A_{0, 0} = 23,$$

$$A_{0, j} = A_{i, 0} = A_{i, -j} = 12 \text{ for } 1 \leq j \leq 4,$$

$$A_{i, j} = 16 \text{ for } 1 \leq i, j \leq 4, \ i \neq j,$$

$$A_{0, 0} = 17,$$

$$A_{0, j} = A_{j, 0} = A_{j, j} = 2 \text{ for } 1 \leq j \leq 9,$$

$$A_{i, j} = 4 \text{ for } 1 \leq i, j \leq 9, \ i \neq j.$$

Here, $A_{i, j}$ denote cyclotomic numbers of order 10. These results obtained
theoretically have been verified by direct computation. This has been done
by setting $\mathbb{F}_{361} = \mathbb{F}_{19}(\sqrt{2})$ and considering the generator $\gamma = 4 + 4\sqrt{2}$ of
$\mathbb{F}_{361}$. Since for any other generator $\gamma' = \gamma^k$, with $ky \equiv 1 \pmod{e}$, we know
that $J_5(i, j)_{\gamma'} = J_5(iy, jy)_{\gamma}$ and $(A_{i, j})_{\gamma'} = (A_{ik, jk})_{\gamma}$, it follows that these
results obtained by computation are independent of the choice of generator.

**Example 2.** Take $p = 5$, $q = p^4 = 625$, $l = 13$. Here, $s = 1$, $f = 4$. By Theorem 2 and Proposition 3, the Jacobi sums of order $e = 13$ and $e = 26$ for the finite field $F_{625}$ are determined to be:

\[
J_e(0, 0) = 623,
J_e(i, 0) = J_e(0, i) = -1 \quad \text{for} \quad 1 \leq i \leq e - 1,
J_e(i, j) = -1 \quad \text{for} \quad 1 \leq i, j \leq e - 1, \quad i + j \equiv 0 \pmod{e},
J_e(i, j) = 25 \quad \text{for} \quad 1 \leq i, j \leq e - 1, \quad i + j \not\equiv 0 \pmod{e}.
\]

From Theorems 4 and 5, the cyclotomic numbers of order 13 and order 26 for the finite field $F_{625}$ are obtained as:

\[
A_{(0, 0)_{13}} = 23,
A_{(0, j)_{13}} = A_{(i, 0)_{13}} = A_{(-j, -j)_{13}} = 2 \quad \text{for} \quad 1 \leq j \leq 12,
A_{(i, j)_{13}} = 4 \quad \text{for} \quad 1 \leq i, j \leq 12, \quad i \not\equiv j,
A_{0, 0} = 23,
A_{0, j} = A_{j, 0} = A_{-j, -j} = 0 \quad \text{for} \quad 1 \leq j \leq 25,
A_{i, j} = 1 \quad \text{for} \quad 1 \leq i, j \leq 25, \quad i \not\equiv j.
\]

Here, $A_{i, j}$ denote cyclotomic numbers of order 26. These results have been verified by direct computation with respect to the generator $\gamma = -x^2 + x^3$ of $F_{625}$, where $f_{625} = F_5(x)$ and $x = \sqrt{2 + \sqrt{2}}$ is a zero of the polynomial $f(x) = x^4 + x^2 + 2$, which is irreducible over the field $F_5$. As seen in Example 1, the Jacobi sums and cyclotomic numbers obtained here by computation are independent of the choice of generator $\gamma$ of $F_{625}^*$.

### 6. SOME APPLICATIONS

In this section, we apply the results of Theorems 4 and 5 to evaluate the number of $F_{q^e}$-rational points on the non-singular projective curves $aY^e = bX^e + cZ^e$ (for $e = l, 2l$ and $abc \neq 0$) defined over any finite field $F_q$ such that $q = p^s \equiv 1 \pmod{e}$ and $p$ is any prime such that ord $p \pmod{l}$ is even.

First, we consider the associated affine curve(s) obtained by setting $Z = 1$ and count the number of $F_{q^e}$-rational points on these curve(s) in terms of the cyclotomic numbers $A_{(i, j)_e}$ of order $e$ for the finite field $F_{q^e}$. Then we
count the points at infinity to obtain the number of $F_{q^n}$-rational points on
the above projective curve(s) in terms of $A(i, j)$. We denote this number by
$a_1(n)$ for $e = l, 2l$ and for each $n \geq 1$. Substituting the values for $A(i, j)$
as obtained in Theorems 4 and 5, we obtain $a_1(n)$ and $a_2(n)$ for each $n \geq 1$.

With these results for $a_i(n)$, we determine the explicit form of the $\zeta$-
fraction of the projective curve $aY^e = bX^e + cZ^e$ defined over $F_q$. Thereby, we
corroborate the Weil conjectures (which have been proved in generality) for
this concrete class of curves given for odd primes $l$.

The Weil conjectures are statements concerning certain properties of the
$\zeta$-function of a non-singular projective variety defined over a finite field.
These are stated in a paper of Weil [11]. These conjectures have been
established in full generality for varieties of dimension $\geq 1$; for a proof of
these conjectures for curves, see [8].

6.1. Counting Points on the Projective Curves $aY^e = bX^e + cZ^e$ ($e = l, 2l$)
over $F_q$

Consider the projective curve(s) $aY^e = bX^e + cZ^e$ ($e = l, 2l$ and $abc \neq 0$)
defined over the finite field $F_q$ where $q = p^n \equiv 1 \pmod{e}$ and $p$ is a prime
such that $\text{ord}_p(e) \equiv 0 \pmod{e}$. Fix a generator $\gamma$ of $F_{q^n}^*$ and let

$$\text{ind}_{\gamma}(b/c) \equiv i \pmod{e} \quad \text{and} \quad \text{ind}_{\gamma}(a/c) \equiv j \pmod{e}.$$ 

Then, for each $n \geq 1$, fix a generator $\beta_n$ of $F_{q^n}$ satisfying
$
\gamma = \beta_n^{(q^n - 1)(q - 1)} = \beta_n^1 + q + \cdots + q^{e-1}.$

Since $q \equiv 1 \pmod{e}$, for each $n \geq 1$ and the finite field $F_{q^n}$, we obtain:

$$\text{ind}_{\beta_n}(b/c) \equiv in \pmod{e} \quad \text{and} \quad \text{ind}_{\beta_n}(a/c) \equiv jn \pmod{e}.$$ 

The number of $F_{q^n}$-rational points on the affine curve $aY^e = bX^e + c$ is
equal to the corresponding number of points on the affine curve $(a/c) Y^e = (b/c) X^e + 1$, and it is not difficult to see that this number is
given by

$$b_e(n) = e^2 A((in, jn)) + \delta(i) + \delta(j),$$

where

$$\delta(r) = \begin{cases} e & \text{if } e | r, \\ 0 & \text{if } e \nmid r. \end{cases}$$

Here, $A((i, j))$ denotes the cyclotomic number of order $e$ for the finite field
$F_{q^n}$. The number of $F_{q^n}$-rational points on the associated projective curve
$(a/c) Y^e = (b/c) X^e + Z^e$ (or equivalently, $aY^e = bX^e + cZ^e$) is then given by

$$a_e(n) = b_e(n) + N,$$
where $N$ is the number of $\mathbb{F}_{q^s}$-rational points at infinity obtained by setting $Z = 0$.

In evaluating $b_s(n)$ and $a_s(n)$, the following cases arise for $in, jn \pmod{e}$ (for each case, we give alongside the corresponding values for $N$ and $a_s(n)$):

(i) \( in, jn \equiv 0 \pmod{e} \), $N = e$, $a_s(n) = e^2A_{(0, 0)} + 3e$,

(ii) \( in \equiv 0 \pmod{e}, jn \not\equiv 0 \pmod{e} \), $N = 0$, $a_s(n) = e^2A_{(0, 0)} + e$,

(iii) \( in \not\equiv 0 \pmod{e}, jn \equiv 0 \pmod{e} \), $N = 0$, $a_s(n) = e^2A_{(0, 0)} + e$,

(iv) \( in, jn \not\equiv 0 \pmod{e} \), \( in \equiv jn \pmod{e} \), $N = e$, $a_s(n) = e^2A_{(0, 0)} + e$,

(v) \( in, jn \not\equiv 0 \pmod{e} \), \( in \not\equiv jn \pmod{e} \), $N = 0$, $a_s(n) = e^2A_{(0, 0)}$.

In the above formulæ for $a_s(n)$, $A_{(a, b)}$ denotes the cyclotomic number of order $e$ for the finite field $\mathbb{F}_{q^s}$. Applying Theorems 4 and 5, we now explicitly obtain the values for $a_l(n)$ and $a_{2l}(n)$ as stated below:

**Theorem 6.** Let $p$ be any prime such that $f = \text{ord } p \pmod{l}$ is even. Let $q = p^s \equiv 1 \pmod{l}$, and $\alpha = fs$ for some integer $s \geq 1$. Consider the projective curve $aY^l = bX^l + cZ^l$ ($abc \neq 0$) defined over the finite field $\mathbb{F}_{q^s}$. Fix any generator $\gamma$ of $\mathbb{F}_{q^s}^*$ and let $\text{ind}_{\gamma}(b/c) \equiv i \pmod{l}$ and $\text{ind}_{\gamma}(a/c) \equiv j \pmod{l}$. Then for each $n \geq 1$, the number $a_l(n)$ of $\mathbb{F}_{q^s}$-rational points on this curve is given as below:

\[
a_l(n) = q^n + 1 - (l - 1)(l - 2)(-1)^m q^{n2}, \quad \text{if} \quad in, jn \equiv 0 \pmod{l},
\]

\[
a_l(n) = q^n + 1 - 2(-1)^m q^{n2}, \quad \text{if} \quad in, jn, in - jn \equiv 0 \pmod{l},
\]

\[
a_l(n) = q^n + 1 + (l - 2)(-1)^m q^{n2}, \quad \text{in all other cases of } in, jn \pmod{l}.
\]

**Theorem 7.** Let $p$ be an odd prime such that $f = \text{ord } p \pmod{l}$ is even. Let $q = p^s \equiv 1 \pmod{2l}$, and $\alpha = fs$ for some integer $s \geq 1$. Consider the projective curve $aY^{2l} = bX^{2l} + cZ^{2l}$ ($abc \neq 0$) defined over the finite field $\mathbb{F}_{q^s}$. Fix any generator $\gamma$ of $\mathbb{F}_{q^s}^*$ and let $\text{ind}_{\gamma}(b/c) \equiv i \pmod{2l}$ and $\text{ind}_{\gamma}(a/c) \equiv j \pmod{2l}$. Then for each $n \geq 1$, the number $a_{2l}(n)$ of $\mathbb{F}_{q^s}$-rational points on this curve is given as below:

\[
a_{2l}(n) = q^n + 1 - (4l^2 - 6l + 2)(-1)^m q^{n2}, \quad \text{if} \quad in, jn \equiv 0 \pmod{2l},
\]

\[
a_{2l}(n) = q^n + 1 - 2(-1)^m q^{n2}, \quad \text{if} \quad in, jn, in - jn \equiv 0 \pmod{2l},
\]

\[
a_{2l}(n) = q^n + 1 + 2(l - 1)(-1)^m q^{n2}, \quad \text{in all other cases of } in, jn \pmod{2l}.
\]
6.2. Zeta Function of the Projective Curve $aY^l = bX^l + cZ^l$ over $F_q$

For an algebraic curve $C$ defined over a finite field $F_q$, the $\zeta$-function of the curve $C$ over $F_q$ is defined as

$$Z(t, C) = Z(t, C/F_q) = \exp \left( \sum_{n=1}^{\infty} \frac{a(n, C)}{n} t^n \right),$$

where $a(n, C)$ is the number of $F_{q^n}$-rational points on $C$.

**Theorem 8.** Consider the projective curve $C: aY^l = bX^l + cZ^l$ ($abc \neq 0$) defined over the finite field $F_q$ where $q = p^s \equiv 1 \pmod{l}$, $p$ is any prime such that $f = \text{ord}_p (\mod{l})$ is even, and $\alpha = f$ for $s \geq 1$. Fix a generator $\gamma$ of $F_q^*$ and let $\text{ind}_\gamma (b/c) \equiv i \pmod{l}$ and $\text{ind}_\gamma (a/c) \equiv j \pmod{l}$. Let $\theta = (-1)^{q^{1/2}}$ and let $\zeta$ be any primitive (complex) $l$th root of unity. Then the $\zeta$-function $Z(t, C)$ of the curve $C$ over $F_q$ is a rational function in the variable $t$, of the form $P(t)/(1-t)(1-qt)$, and the polynomial $P(t)$ is given explicitly as follows:

1. For $i, j \equiv 0 \pmod{l}$,
   $$P(t) = (1 - \theta t)^{l-1}(l-2).$$

2. For
   (i) $i \equiv 0 \pmod{l}$, $j \not\equiv 0 \pmod{l}$,
   (ii) $i \not\equiv 0 \pmod{l}$, $j \equiv 0 \pmod{l}$, and
   (iii) $i, j \not\equiv 0 \pmod{l}$, $i \equiv j \pmod{l}$,
   $$P(t) = (1 + \theta t + \theta^2 t^2 + \ldots + \theta^{l-1}t^{l-1})^{l-2} = \prod_{r=1}^{l-1} (1 - \zeta^r \theta t)^{l-2}.$$

3. For $i, j, i-j \not\equiv 0 \pmod{l}$,
   $$P(t) = (1 - \theta t)^{l-1}(1 + \theta t + \ldots + \theta^{l-1}t^{l-1})^{l-3}$$
   $$= (1 - \theta t)^{l-1} \prod_{r=1}^{l-1} (1 - \zeta^r \theta t)^{l-3}.$$
1. For \( i, j \equiv 0 \pmod{l} \),

\[
\log Z(t, C) = \sum_{n=1}^{\infty} \frac{(q^n + 1 - (l-1)(l-2)(-1)^m q^{n/2}) t^n}{n}
\]

\[
= \sum_{n=1}^{\infty} \frac{q^n t^n}{n} + \sum_{n=1}^{\infty} \frac{t^n}{n} - (l-1)(l-2) \sum_{n=1}^{\infty} \frac{(-1)^m q^{n/2} t^n}{n}
\]

\[
= \log \frac{1}{1-qt} + \log \frac{1}{1-t} - (l-1)(l-2) \log \frac{1}{1-(-1)^m q^{1/2} t}
\]

Thus

\[
Z(t, C) = \frac{1 - (1)^m q^{1/2} t^{(l-1)(l-2)}}{(1-t)(1-qt)}
\]

2. For

(i) \( i \equiv 0 \pmod{l}, j \not\equiv 0 \pmod{l} \),

(ii) \( i \not\equiv 0 \pmod{l}, j \equiv 0 \pmod{l} \), and

(iii) \( i, j \not\equiv 0 \pmod{l}, i \equiv j \pmod{l} \),

\[
\log Z(t, C) = \sum_{n=1}^{\infty} \frac{(q^n + 1 - (l-2)(-1)^m q^{n/2}) t^n}{n}
\]

\[
+ \sum_{n=1}^{\infty} \frac{(q^n + 1 - (l-1)(l-2)(-1)^{2m} q^{n/2}) t^n}{l n}
\]

\[
- \sum_{n=1}^{\infty} \frac{(q^n + 1 - (l-2)(-1)^{2m} q^{n/2}) t^n}{l n}
\]

\[
= \sum_{n=1}^{\infty} \frac{q^n t^n}{n} + \sum_{n=1}^{\infty} \frac{t^n}{n} + (l-2) \sum_{n=1}^{\infty} \frac{(-1)^m q^{n/2} t^n}{n}
\]

\[
- l(l-2) \sum_{n=1}^{\infty} \frac{(-1)^{2m} q^{n/2} t^n}{l n}
\]

\[
= \log \frac{1}{1-qt} + \log \frac{1}{1-t} + (l-2) \log \frac{1}{1-(-1)^m q^{1/2} t}
\]

\[
- (l-2) \log \frac{1}{1-(-1)^m q^{1/2} t}.
\]
Hence
\[ Z(t, C) = \frac{(1 - (-1)^{\beta} q^{1/2} t)^{l-2}}{(1-t)(1-qt)(1-(-1)^{\sigma} q^{1/2} t)^{l-2}} = \frac{(1 + \theta t + \theta^2 t^2 + \cdots + \theta^{l-1} t^{l-1})^{l-2}}{(1-t)(1-qt)}. \]

3. For \( i, j, i-j \not\equiv 0 \pmod{l} \),

\[ \log Z(t, C) = \sum_{n=1}^{\infty} \frac{(q^n + 1 - 2(-1)^{\nu_n} q^{n/2}) t^n}{n} \]
\[ + \sum_{n=1}^{\infty} \frac{(q^n + 1 - (l-1)(l-2)(-1)^{\nu_n} q^{n/2}) t^n}{ln} \]
\[ - \sum_{n=1}^{\infty} \frac{(-1)^{\nu_n} q^{n/2} t^n}{ln} \]
\[ = \sum_{n=1}^{\infty} q^n t^n + \sum_{n=1}^{\infty} \frac{t^n}{n} - 2 \sum_{n=1}^{\infty} \frac{(-1)^{\nu_n} q^{n/2} t^n}{ln} \]
\[ - (l-3) \sum_{n=1}^{\infty} \frac{(-1)^{\nu_n} q^{n/2} t^n}{ln} \]
\[ = \log \frac{1}{1-qt} + \log \frac{1}{1-t} - 2 \log \frac{1}{1-(-1)^{\nu} q^{1/2} t} \]
\[ - (l-3) \log \frac{1}{1-(-1)^{\nu} q^{1/2} t}. \]

It follows that
\[ Z(t, C) = \frac{(1 - (-1)^{\nu} q^{1/2} t)^2 (1 - (-1)^{\beta} q^{1/2} t)^{l-3}}{(1-t)(1-qt)} = \frac{(1-\theta t)^{l-1} (1+\theta t + \cdots + \theta^{l-1} t^{l-1})^{l-3}}{(1-t)(1-qt)}. \]

Hence the theorem.

The curve \( C \) considered in Theorem 8 is non-singular of degree \( l \); hence it has genus \( g = ((l-1)(l-2))/2 \). It is clear that for each case of \( i, j \pmod{l} \), the polynomial \( P(t) \) (in the Theorem) is of degree \( 2g \) and has integral coefficients with leading term \( q^g \) and constant term 1. (Note that \( q^{1/2} \) is an integer.) Further, if we write

\[ P(t) = \prod_{k=1}^{2g} (1-\sigma_k t), \quad 2g = (l-1)(l-2), \]
it is clear that in each case we may pair the $x_k$ in such a way that
$x_k x_{k+m} = q$ for $1 \leq k \leq g$, and $|x_k| = g^{1/2}$ for $1 \leq k \leq 2g$. Thus the Weil conjectures are corroborated for this concrete class of curves $C$.

Remarks. (1) In Theorem 7, we have obtained the number of $F_q$-rational points on the non-singular projective curve $aY^2 = bX^2 + cZ^2$ defined over certain finite fields $F_q$. As in Theorem 8 of this paper, we may similarly obtain the explicit form of the $\zeta$-function for the above curve over $F_q$, and thereby verify the Weil conjectures in this concrete case. Here, one has to consider various distinct cases of $a$, $b$, and $c$ in $F_q$; the explicit $\zeta$-functions for these cases will be obtained in a separate paper.

(2) The Jacobsthal sums $\phi_j(v)$ and the related sums $\psi_j(v)$ of order $e$ over a finite field $F_q$ ($v \in F_q$) are known to be useful in evaluating the number of points on curves of the form $aY^2 = bX^2 + c$ ($abc \neq 0$) defined over $F_q$. For odd primes $p$ and $l$, the Jacobsthal sums $\phi_j(v)$ of order $l$ over $F_q$, $q = p^s \equiv 1 \pmod{l}$, have been obtained in terms of the coefficients of the Jacobi sum $J_l(1, 1)$ of order $l$ for this field (see [6]). The sums $\psi_j(v)$ and $\psi_{2j}(v)$ for this field are then given in terms of the sums $\phi_j(v)$. Thus for odd primes $p$, $l$ such that $ord\, p \pmod{l}$ is even, and $q = p^s \equiv 1 \pmod{l}$, we may apply the results of Theorem 2 in this paper to determine explicitly the sums $\phi_j(v)$, $\psi_j(v)$, and $\psi_{2j}(v)$ for the finite field $F_q$. The explicit values for these sums may then be applied to determine the exact number of points on the affine curves $aY^2 = bX^2 + c$ and $aY^2 = bX^2 + c$ ($abc \neq 0$) defined over $F_q$, in terms of $q$ and $l$. Thereby, one may obtain the explicit form of $\zeta$-functions of the associated projective curves defined over $F_q$. Interestingly, the Weil conjectures (stated for non-singular projective curves) continue to hold true for the $\zeta$-function of the former projective curve, viz. $aY^2Z^{l-2} = bX^2 + cZ^2$, even for odd primes $l > 3$ for which this curve is singular. This work will be treated separately.

ACKNOWLEDGMENTS

The first author thanks the Council for Scientific and Industrial Research, India, for support received in the form of a research fellowship. The authors also thank the referee for carefully going through the manuscript and suggesting some modifications in the format.

REFERENCES