Chapter 4

Gaussian Hypergeometric Series
and \( y^\ell = (x - 1)(x^2 + \lambda) \)

4.1 Introduction

Finding number of solutions of a polynomial equation over a finite field has been of interest to mathematicians for many years. Recently, lots of progress have been made to express the number of \( \mathbb{F}_q \)-points on certain families of algebraic curves in terms of Gaussian hypergeometric functions. For example, Fuselier [14], Koike [25], Lennon [27, 28], and Ono [34] expressed the traces of Frobenius of certain families of elliptic curves in terms of particular values of Gaussian hypergeometric series. In Chapter 2, we have also discussed this problem for certain families of elliptic curves, and extend some of the earlier results. Moreover, Vega [40] connected the number of points on an algebraic curve of degree \( \ell > 0 \) in \( \mathbb{F}_q \) with Gaussian hypergeometric series.

Let \( \ell \geq 2, \) and \( f(x) \) be a cubic polynomial over \( \mathbb{Q} \). In Chapter 3, we considered the algebraic curve \( y^\ell = x(x - 1)(x - \lambda) \) and found relations between the number of points on the algebraic curve and hypergeometric series over finite fields. In this chapter, we consider the algebraic curve \( y^\ell = (x - 1)(x^2 + \lambda) \). For this family of algebraic curves, we give relations between the number of \( \mathbb{F}_q \)-points on the algebraic curve and \( {}_2F_1 \) and \( {}_3F_2 \) Gaussian hypergeometric series, separately. We also provide

\[ {}_2F_1 \quad \text{and} \quad {}_3F_2 \]

The contents of this chapter have appeared in *Int. J. Number Theory* (2012).

49
an alternate proof of a result of McCarthy [30].

4.2 Preliminaries

First of all, we restate some results of Evans and Greene from [11, 12], which will be used to prove our results. In [12], for \( A, B \in \overline{\mathbb{F}}_q^\times \) the function \( F(A, B; x) \) is defined by

\[
F(A, B; x) := \frac{q}{q - 1} \sum_\chi \left( A\chi^2 \right) \left( A\chi \right) \chi \left( \frac{x}{4} \right),
\]

(4.2.1)

and its normalization as

\[
F^*(A, B; x) := F(A, B; x) + AB(-1) \frac{\overline{A}(x)}{q}.
\]

(4.2.2)

Another character sum from [11] that we will need is

\[
g(A, B; x) := \sum_{t \in \mathbb{F}_q} A(1 - t)B(1 - xt^2), \quad x \in \mathbb{F}_q.
\]

(4.2.3)

There is a nice relationship between the two functions \( F^*(A, B; x) \) and \( g(A, B; x) \) stated as follows.

**Theorem 4.2.1.** [11, Thm. 2.2] If \( A \neq C \) and \( x \notin \{0, 1\} \), then

\[
F^* \left( A, C; \frac{x}{x - 1} \right) = \frac{A(2)A\overline{C}(1 - x)}{q} \cdot g(A\overline{C}^2, A\overline{C}; 1 - x).
\]

Further, the following theorems give connections of the functions \( F^*(A, B; x) \) and \( g(A, B; x) \) with Gaussian hypergeometric series.

**Theorem 4.2.2.** [11, Thm. 2.5] Let \( C \neq \phi, A \notin \{\varepsilon, C, C^2\} \), \( x \neq 1 \). Then

\[
\begin{aligned}
3\text{F}_2 \left( \begin{array}{c} A, \overline{A}C^2, C\phi \\ C^2, C \end{array} \mid x \right) &= - \frac{\overline{C}(x)\phi(1 - x)}{q} + C(-1)A\overline{C}(4)A\overline{C}^2(1 - x) \times \\
& \quad \frac{J(A\overline{C}^2, A\overline{C})}{q^2J(A, A\overline{C})} \cdot g(A\overline{C}^2, A\overline{C}; 1 - x)^2.
\end{aligned}
\]
Theorem 4.2.3. [12, Thm. 1.2] Let $R^2 \notin \{\varepsilon, C, C^2\}$. Then

$$F^*(R^2, C; x) = R(4) \frac{J(\phi, CR^2)}{J(RC, R\phi)} \cdot 2F_1 \left( \begin{array}{c} R\phi, \; R \\ C \end{array} \right).$$

We now prove a result similar to the above theorem.

Proposition 4.2.4. We have

$$F^*(\varepsilon, C; x) = \begin{cases} 2F_1 \left( \begin{array}{c} \phi, \; \varepsilon \\ C \end{array} \right), & \text{if } C \neq \varepsilon; \\ -(q-2) \cdot 2F_1 \left( \begin{array}{c} \phi, \; \varepsilon \\ C \end{array} \right), & \text{if } C = \varepsilon. \end{cases}$$

Proof. We prove the result following the technique used in [12]. From [18, (4.21)], we know that

$$\begin{pmatrix} B^2 \chi^2 \\ \chi \end{pmatrix} = \begin{pmatrix} \phi B \chi \\ \chi \end{pmatrix} \begin{pmatrix} B \chi \\ B^2 \chi \end{pmatrix} \left( \begin{array}{c} \phi \\ \phi B \end{array} \right)^{-1} B \chi(4).$$

Putting $B = \varepsilon$, we have

$$\begin{pmatrix} \chi^2 \\ \chi \end{pmatrix} = \begin{pmatrix} \phi \chi \\ \chi \end{pmatrix} \begin{pmatrix} \chi \\ \chi \end{pmatrix} \left( \begin{array}{c} \phi \\ \phi \end{array} \right)^{-1} \chi(4). \tag{4.2.4}$$

From (4.2.4) and (4.2.1), we obtain

$$F(\varepsilon, C; x) = \frac{q}{q-1} \sum_{\chi} \begin{pmatrix} \chi^2 \\ \chi \end{pmatrix} \begin{pmatrix} \chi \\ C\chi \end{pmatrix} \chi \left( \begin{array}{c} x \\ q \end{array} \right)$$

$$= \frac{q}{q-1} \sum_{\chi} \begin{pmatrix} \chi \\ C\chi \end{pmatrix} \left( \begin{array}{c} \phi \chi \\ \chi \end{array} \right) \left( \begin{array}{c} \phi \\ \phi \end{array} \right)^{-1} \chi(4) \chi \left( \begin{array}{c} x \\ q \end{array} \right)$$

$$= \left( \begin{array}{c} \phi \end{array} \right)^{-1} \begin{pmatrix} 3F_2 \left( \begin{array}{c} \phi, \; \varepsilon, \; \varepsilon \\ C, \; \varepsilon \end{array} \right) \right). \tag{4.2.5}$$

By Theorem 1.3.13, (4.2.5) reduces to

$$\begin{pmatrix} \phi \\ \phi \end{pmatrix} F(\varepsilon, C; x) = \begin{pmatrix} C \end{array} \right) 2F_1 \left( \begin{array}{c} \phi, \; \varepsilon \\ C \end{array} \right) - \frac{C(-1)^q \phi \chi(4)}{q} \chi. \tag{4.2.6}$$
From (4.2.2), we have
\[
\left(\frac{\phi}{\phi}\right) F(\varepsilon, C; x) = \left(\frac{\phi}{\phi}\right) F^*(\varepsilon, C; x) - \frac{C(-1)}{q} \left(\frac{\phi}{\phi}\right) .
\] (4.2.7)

Comparing equations (4.2.6) and (4.2.7), we obtain
\[
F^*(\varepsilon, C; x) = \left(\frac{C}{C}\right) \left(\frac{\phi}{\phi}\right)^{-1} _2F_1 \left( \begin{array}{c} \varepsilon \\ C \end{array} \right | x \right).
\]

Using (1.3.2), we complete the proof of the result. \qed

4.3 Main results

Let \( \lambda \in \mathbb{Q} \setminus \{0, -1\} \) and \( \ell \geq 2 \). Denote by \( V_{\ell, \lambda} \) the nonsingular projective algebraic curve over \( \mathbb{Q} \) with affine equation given by
\[
y^\ell = (x - 1)(x^2 + \lambda).
\] (4.3.1)

Remark 4.3.1. If \( \ell = 3 \), \( V_{3, \lambda} \) is an elliptic curve. The change of variables

\[
X - Z \rightarrow X, \; Y \rightarrow Y \; \text{and} \; X \rightarrow X
\]

transforms the projective curve

\[
V_{3, \lambda} : Y^3 = (X - Z)(X^2 + \lambda Z^2)
\]

to

\[
Y^3 = X(X^2 + 2XZ + (1 + \lambda)Z^2).
\] (4.3.2)

Now dehomogenizing (4.3.2) by putting \( X = 1 \) and then making the substitution
\[
Y \rightarrow (1 + \lambda)x, \; Z \rightarrow (1 + \lambda)y - \frac{1}{1 + \lambda},
\]

we find that \( V_{3, \lambda} \) is isomorphic over \( \mathbb{Q} \) to the elliptic curve
\[
y^2 = x^3 - \frac{\lambda}{(1 + \lambda)^4}.
\]
We now define an integer \( a_q(V_{\ell,\lambda}) \) analogous to the trace of Frobenius of elliptic curves.

**Definition 4.3.1.** Suppose \( p \) is a prime of good reduction for \( V_{\ell,\lambda} \). Let \( q = p^e \). Define the integer \( a_q(V_{\ell,\lambda}) \) by

\[
a_q(V_{\ell,\lambda}) := 1 + q - \#V_{\ell,\lambda}(\mathbb{F}_q),
\]

where \( \#V_{\ell,\lambda}(\mathbb{F}_q) \) denotes the number of points that the curve \( V_{\ell,\lambda} \) has over \( \mathbb{F}_q \).

It is clear that a prime \( p \) not dividing \( \ell \) is of good reduction for \( V_{\ell,\lambda} \) if and only if \( \text{ord}_p(\lambda(\lambda + 1)) = 0 \).

Similar to the Remark 3.2.3, we have the following remark regarding the number of \( \mathbb{F}_q \)-points on \( V_{\ell,\lambda} \). For details, see Remark 3.2.3.

**Remark 4.3.2.** Let \( \ell \neq 3 \). Then

\[
\#V_{\ell,\lambda}(\mathbb{F}_q) = 1 + \#\{(x, y) \in \mathbb{F}_q^2 : y^\ell = (x - 1)(x^2 + \lambda)\}.
\]  

(4.3.3)

In fact, for \( \ell \geq 4 \), the point \([1 : 0 : 0]\) is the only point at infinity. Moreover, if \( \ell = 2 \), the point at infinity is \([0 : 1 : 0]\).

Further, let \( \ell = 3 \) and \( p \equiv 1 \pmod{3} \). Consider \( \omega \in \mathbb{F}_q^\times \) be of order 3. Then there are three points at infinity of \( V_{\ell,\lambda} \), namely \([1 : 1 : 0]\), \([1 : \omega : 0]\), and \([1 : \omega^2 : 0]\). Hence,

\[
\#V_{\ell,\lambda}(\mathbb{F}_q) = 3 + \#\{(x, y) \in \mathbb{F}_q^2 : y^\ell = (x - 1)(x^2 + \lambda)\}.
\]  

(4.3.4)

Again, if \( \ell = 3 \) and \( p \equiv 2 \pmod{3} \), the only point at infinity is \([1 : 1 : 0]\).
4.3.1 \( y^\ell = (x - 1)(x^2 + \lambda) \) and \( 3F_2 \) Gaussian hypergeometric series

Ono [34, Thm. 5], proved that if \( \lambda \in \mathbb{Q} \setminus \{0, -1\} \) and \( p \) is an odd prime for which \( \text{ord}_p(\lambda(\lambda + 1)) = 0 \) then

\[
3F_2 \left( \frac{\phi, \phi, \phi}{\varepsilon, \varepsilon} \Bigg| \frac{1 + \lambda}{\lambda} \right) = \frac{\phi(-\lambda)(a_p(V_{2,\lambda})^2 - p)}{p^2}.
\]  

(4.3.5)

Note that a change of variables in Theorem 5 of Ono [34] is required to arrive at (4.3.5). In this chapter, we give a proof of the following result which generalizes (4.3.5) to the algebraic curve \( V_{\ell,\lambda} \) over \( \mathbb{F}_q \).

**Theorem 4.3.1.** Let \( p \) be a prime such that \( \text{ord}_p(\lambda(\lambda + 1)) = 0 \) and \( q = p^e \equiv 1 \pmod{\ell} \). If \( \ell \geq 2 \) is such that \( 3 \nmid \ell \) or \( 4 \nmid \ell \), then

\[
a_q(V_{\ell,\lambda})^2 = q^2 \cdot \sum_{i=1}^{\ell-1} \frac{J(S^{3i}, S^{-i})}{S^i(-4\lambda^3)J(S^i, S^i)} \cdot 3F_2 \left( \frac{S^{3i}, S^i, S^{2i}\phi}{S^{4i}, S^{2i}} \Bigg| \frac{1 + \lambda}{\lambda} \right)
\]

\[
+ q \cdot \sum_{i=1}^{\ell-1} \frac{\phi(-\lambda)J(S^{3i}, S^{-i})}{S^i(-4\lambda(1 + \lambda)^2)J(S^i, S^i)} + Q,
\]

where

\[
Q = \begin{cases} 
(\ell - 1)(q - 1) - (\ell - 3)a_q(V_{\ell,\lambda}), & \text{if } \ell \text{ is odd;} \\
(\ell - 2)(q - 1) - (\ell - 2)a_q(V_{\ell,\lambda}) \\
-2q \cdot \sum_{i=1}^{\ell-1} \frac{J(\phi, S^{-2i})}{J(S^i\phi, S^{-3i})} \cdot 2F_1 \left( \frac{S^{3i}, S^{3i}\phi}{S^{4i}} \Bigg| 1 + \lambda \right), & \text{if } \ell \text{ is even}
\end{cases}
\]

and \( S \) is a character on \( \mathbb{F}_q \) of order \( \ell \).

**Proof.** Putting \( A = S^i, B = S^i \) and \( x = -\frac{1}{\lambda} \) in (4.2.3), we obtain

\[
g \left( S^i, S^i, -\frac{1}{\lambda} \right) = \sum_{t \in \mathbb{F}_q} S^{-i}(-\lambda)S^i((t - 1)(t^2 + \lambda))
\]
which gives
\[
\sum_{t \in \mathbb{F}_q} S^i((t - 1)(t^2 + \lambda)) = S^i(-\lambda) g \left( S^i, S^i; -\frac{1}{\lambda} \right). \tag{4.3.6}
\]

Moreover,
\[
\# \{(x, y) \in \mathbb{F}_q^2 : y^\ell = (x - 1)(x^2 + \lambda)\}
= \sum_{t \in \mathbb{F}_q} \# \{y \in \mathbb{F}_q : y^\ell = (t - 1)(t^2 + \lambda)\}
= \sum_{t \in \mathbb{F}_q, (t - 1)(t^2 + \lambda) \neq 0} \# \{y \in \mathbb{F}_q : y^\ell = (t - 1)(t^2 + \lambda)\} + \# \{t \in \mathbb{F}_q : (t - 1)(t^2 + \lambda) = 0\}.
\]

Applying Lemma 1.3.6, we obtain
\[
\# \{(x, y) \in \mathbb{F}_q^2 : y^\ell = (x - 1)(x^2 + \lambda)\}
= \sum_{t \in \mathbb{F}_q} \sum_{i = 0}^{\ell - 1} S^i((t - 1)(t^2 + \lambda)) + \# \{t \in \mathbb{F}_q : (t - 1)(t^2 + \lambda) = 0\}
= q + \sum_{t \in \mathbb{F}_q} \sum_{i = 1}^{\ell - 1} S^i((t - 1)(t^2 + \lambda)).
\]

Since \(\text{ord}_p(\lambda(\lambda + 1)) = 0\), (4.3.3) yields
\[
-a_q(V_{\ell,\lambda}) = \sum_{i = 1}^{\ell - 1} \sum_{t \in \mathbb{F}_q} S^i((t - 1)(t^2 + \lambda)). \tag{4.3.7}
\]

Squaring both sides of (4.3.7), we obtain
\[
a_q(V_{\ell,\lambda})^2 = \sum_{i = 1}^{\ell - 1} \left[ \sum_{t \in \mathbb{F}_q} S^i((t - 1)(t^2 + \lambda)) \right]^2 + \sum_{i,j = 1, i \neq j}^{\ell - 1} \sum_{t \in \mathbb{F}_q} S^{i+j}((t - 1)(t^2 + \lambda)).
\]

Again using (4.3.6), we deduce that
\[
a_q(V_{\ell,\lambda})^2 = \sum_{i = 1}^{\ell - 1} S^i(\lambda^2) g \left( S^i, S^i; -\frac{1}{\lambda} \right)^2 + \sum_{i,j = 1, i \neq j, i + j = \ell}^{\ell - 1} \sum_{t \in \mathbb{F}_q} S^{i+j}((t - 1)(t^2 + \lambda))
+ \sum_{i,j = 1, i \neq j, i + j \neq \ell}^{\ell - 1} \sum_{t \in \mathbb{F}_q} S^{i+j}((t - 1)(t^2 + \lambda)).
\]
Then Lemma 1.3.7 yields
\[ a_q(V_{\ell,\lambda})^2 = \sum_{i=1}^{\ell-1} S^i(\lambda^2)g\left(S^i, S^i; -\frac{1}{\lambda}\right)^2 + 2(q - 1) \cdot \left\lfloor \frac{\ell - 1}{2} \right\rfloor \]
\[ + \sum_{i,j=1, i \neq j, i+j \neq \ell \in \mathbb{F}_q} S^{i+j}((t-1)(t^2 + \lambda)). \] (4.3.8)

Since \(3 \nmid \ell\) or \(4 \nmid \ell\), taking \(A = S^{-3i}, C = S^{-2i}\) and \(x = \frac{1+\lambda}{\lambda}\) in Theorem 4.2.2, we obtain
\[ g\left(S^i, S^i; -\frac{1}{\lambda}\right)^2 = q^2 \cdot \frac{S^i(-4\lambda)J(S^{-3i}, S^i)}{J(S^{-i}, S^{-i})} \cdot 3F_2 \left( \begin{array}{c} S^{-3i}, S^{-i}, S^{-2i}\phi \mid 1 + \lambda \\ S^{-4i}, S^{-2i} \end{array} \right) \]
\[ + q \cdot \frac{\phi(-\lambda)S^i(-\frac{4(1+\lambda)^2}{\lambda})J(S^{-3i}, S^i)}{J(S^{-i}, S^{-i})}. \] (4.3.9)

Now we find the value of
\[ \sum_{i,j=1, i \neq j, i+j \neq \ell \in \mathbb{F}_q} S^{i+j}((t-1)(t^2 + \lambda)). \]

Let \(P(i_k)\) be the set of all possible values of \(i\) such that \(i + j \equiv k \pmod{\ell}\), \(1 \leq i, j \leq \ell - 1\) and \(i \neq j\). Then for odd values of \(\ell\)
\[ \#P(i_k) = \ell - 3 \]
and for even values of \(\ell\)
\[ \#P(i_k) = \begin{cases} \ell - 2, & \text{if } \ell \text{ is odd;} \\ \ell - 4, & \text{if } \ell \text{ is even.} \end{cases} \]

Therefore,
\[ \sum_{i,j=1, i \neq j, i+j \neq \ell \in \mathbb{F}_q} S^{i+j}((t-1)(t^2 + \lambda)) \]
\[ = \begin{cases} (\ell - 3) \sum_{i=1}^{\ell-1} \sum_{t \in \mathbb{F}_q} S^i((t-1)(t^2 + \lambda)), & \text{if } \ell \text{ is odd;} \\ (\ell - 2) \sum_{i=1}^{\ell-1} \sum_{t \in \mathbb{F}_q} S^i((t-1)(t^2 + \lambda)) - 2 \sum_{i=1}^{\ell-1} \sum_{t \in \mathbb{F}_q} S^{2i}((t-1)(t^2 + \lambda)), & \text{if } \ell \text{ is even.} \end{cases} \]
From (4.3.7), (4.2.3) and Theorem 4.2.1, we deduce that

\[
\sum_{i,j=1, i \neq j, i+j \neq \ell} S^{i+j} ((t-1)(t^2+\lambda))
\]

\[
= \begin{cases} 
-(\ell-3)a_q(V_{\ell,\lambda}), & \text{if } \ell \text{ is odd;} \\
-(\ell-2)a_q(V_{\ell,\lambda}) \\
-2q \sum_{i=1}^{\frac{\ell-1}{2}} \frac{J(\phi, S^{2i})}{J(S^{-i}, S^{3i}\phi)} \cdot _2F_1 \left( \begin{array}{c} S^{-3i}\phi, \ S^{-3i} \\
S^{-4i} \end{array} \mid 1+\lambda \right), & \text{if } \ell \text{ is even.}
\end{cases}
\]

(4.3.10)

Using (4.3.9) and (4.3.10) in (4.3.8), we complete the proof.

\[\square\]

Remark 4.3.3. Putting \(\ell = 2\) in Theorem 4.3.1, we obtain

\[
a_q(V_{2,\lambda})^2 = q^2 \phi(-\lambda) \cdot _3F_2 \left( \begin{array}{c} \phi, \ \phi, \ \phi \\
\varepsilon, \ \varepsilon \end{array} \mid \frac{1+\lambda}{\lambda} \right) + q, \quad (4.3.11)
\]

which yields (4.3.5) over \(\mathbb{F}_q\).

4.3.2 \(y^\ell = (x-1)(x^2+\lambda)\) and \( _2F_1 \) Gaussian hypergeometric series

In the previous subsection, we have expressed the number of \(\mathbb{F}_q\)-points on the algebraic curve \(V_{\ell,\lambda}\) as linear combination of \(_3F_2\) Gaussian hypergeometric function.

Now, we prove the following result, which connects the number of points on \(V_{\ell,\lambda}\) and \(_2F_1\) hypergeometric series over \(\mathbb{F}_q\).

Theorem 4.3.2. Suppose that \(q = p^e \equiv 1 \pmod{\ell}\) and \(\text{ord}_p(\lambda(\lambda+1)) = 0\). If \(3 \nmid \ell\) and \(\frac{q-1}{\ell}\) is even, then

\[
-a_q(V_{\ell,\lambda}) = q \cdot \sum_{i=1}^{\ell-1} \frac{J(\phi, S^{-i})}{J(\sqrt{S^i}, \sqrt{S^{-3i}\phi})} \cdot _2F_1 \left( \begin{array}{c} \sqrt{S^{3i}}\phi, \ \sqrt{S^{3i}} \\
S^{2i} \end{array} \mid 1+\lambda \right) \quad (4.3.12)
\]
and for $\ell = 3$,

$$-a_q(V_{t,\lambda}) = 2 + q \cdot \sum_{i=1}^{2} F_1 \left( \phi, \frac{\varepsilon}{S^i} | 1 + \lambda \right), \quad (4.3.13)$$

where $S$ is a character of order $\ell$ on $\mathbb{F}_q$.

**Proof.** Following the proof of Theorem 4.3.1, we obtain

$$\sum_{t \in \mathbb{F}_q} S^i((t - 1)(t^2 + \lambda)) = S^i(-\lambda)g \left( S^i, S^i; -\frac{1}{\lambda} \right) \quad (4.3.14)$$

and

$$\# \{ (x, y) \in \mathbb{F}_q^2 : y^\ell = (x - 1)(x^2 + \lambda) \} = q + \sum_{i=1}^{\ell - 1} \sum_{t \in \mathbb{F}_q} S^i((t - 1)(t^2 + \lambda)). \quad (4.3.15)$$

Since $S^i \neq \varepsilon$, we have $S^{-2i} \neq S^{-3i}$. Putting $A = S^{-3i}$, $C = S^{-2i}$ and $x = \frac{1 + \lambda}{\lambda}$ in Theorem 4.2.1, we deduce that

$$g(S^i, S^i; -\frac{1}{\lambda}) = qS^i\left( -\frac{8}{\lambda} \right) F^*(S^{-3i}, S^{-2i}; 1 + \lambda). \quad (4.3.16)$$

As $\frac{\ell - 1}{\ell}$ is even, $S^i$ is a square. Also, $3 \nmid \ell$ implies that $S^i \neq \varepsilon$. So applying Theorem 4.2.3, we obtain

$$g(S^i, S^i; -\frac{1}{\lambda}) = \frac{qS^i\left( -\frac{1}{\lambda} \right) J(\phi, S^i)}{J(\sqrt{S^{-3i}}, \sqrt{S^{3i}})} \cdot 2F_1 \left( \sqrt{S^{-3i}} \phi, \sqrt{S^{-3i}} S^{-2i} | 1 + \lambda \right). \quad (4.3.17)$$

From (4.3.14), (4.3.15), and (4.3.17), we have

$$\# \{ (x, y) \in \mathbb{F}_q^2 : y^\ell = (x - 1)(x^2 + \lambda) \}$$

$$= q + \sum_{i=1}^{\ell - 1} S^i(-\lambda)g \left( S^i, S^i; -\frac{1}{\lambda} \right)$$

$$= q + q \cdot \sum_{i=1}^{\ell - 1} \frac{J(\phi, S^i)}{J(\sqrt{S^{-2i}}, \sqrt{S^{2i}})} \cdot 2F_1 \left( \sqrt{S^{-3i}} \phi, \sqrt{S^{-3i}} S^{-2i} | 1 + \lambda \right).$$

Since $\text{ord}_p(\lambda(\lambda + 1)) = 0$, (4.3.3) completes the proof of (4.3.12).
Again, if \( \ell = 3 \), then \( S_{-3i} = \varepsilon \) and \( S_{-2i} = S^i \). Therefore, using Proposition 4.2.4 in (4.3.16), we obtain
\[
g(S^i, S^i; -\frac{1}{\lambda}) = qS^i((-\frac{8}{\lambda})F^*(\varepsilon, S^i; 1 + \lambda)) = qS^i(-\frac{1}{\lambda})2F_1\left( \begin{array}{c} \phi \varepsilon \\ S^i \\ 1 + \lambda \end{array} \right) \tag{4.3.18}
\]

Now combining (4.3.18) with (4.3.14) and (4.3.15), we deduce that
\[
\#\{(x, y) \in \mathbb{F}_q^2 : y^\ell = (x - 1)(x^2 + \lambda)\} = q + \sum_{i=1}^{\ell-1} S^i(-\lambda)g\left( S^i, S^i; -\frac{1}{\lambda} \right)
\]
\[
= q + q \sum_{i=1}^{2} 2F_1\left( \begin{array}{c} \phi \varepsilon \\ S^i \\ 1 + \lambda \end{array} \right)
\]
which yields the result because of (4.3.4).

**Corollary 4.3.3.** Let \( p \) be an odd prime for which \( \text{ord}_p(\lambda(\lambda+1)) = 0 \). If \( p \equiv 1 \pmod{3} \) and \( x^2 + 3y^2 = p \), then
\[
a_p(V_{3, \frac{-1}{2}}) = \phi(2)(-1)^{x+y-1}\left( \frac{x}{3} \right) \cdot 2x
\]
and
\[
p \cdot 2 \sum_{i=1}^{2} 2F_1\left( \begin{array}{c} \phi \varepsilon \\ \chi_3^i \\ \frac{1}{2} \end{array} \right) = \phi(2)(-1)^{x+y}\left( \frac{x}{3} \right) \cdot 2x - 2,
\]
where \( \chi_3 \) is a character on \( \mathbb{F}_p \) of order 3.

**Proof.** As mentioned in Remark 4.3.1, \( V_{3, \frac{-1}{2}} \) is isomorphic over \( \mathbb{Q} \) to the elliptic curve
\[
E : y^2 = x^3 + 2^3,
\]
which is 2-quadratic twist of \( E' : y^2 = x^3 + 1 \). It is known that if \( E(d) \) is the \( d \)-quadratic twist of the elliptic curve \( E \) and \( \gcd(p, d) = 1 \), then
\[
a_p(E) = \phi(d)a_p(E(d)).
\]
Again, from [34, Prop. 2], we have
\[ a_p(E') = (-1)^{x+y-1} \left( \frac{x}{3} \right) \cdot 2x. \]
Since \( \gcd(p, 2) = 1 \), we must have
\[ a_p(V_{3, -\frac{1}{2}}) = \phi(2)a_p(E') \]
\[ = \phi(2)(-1)^{x+y-1} \left( \frac{x}{3} \right) \cdot 2x. \quad (4.3.19) \]

Again combining this result with the equation \((4.3.13)\), we complete the second part of the corollary.

Now, we have the following corollary which is the finite field analog of a particular case of the Clausen Theorem of classical hypergeometric series.

**Corollary 4.3.4.** Let \( p \) be an odd prime for which \( \text{ord}_p(\lambda(\lambda + 1)) = 0 \). If \( q = p^e \equiv 1 \pmod{4} \), then
\[ _3F_2 \left( \phi, \phi, \phi \left| \frac{1 + \lambda}{\lambda} \right. \right) = \phi(\lambda) _2F_1 \left( \left. \frac{\chi_4}{\varepsilon}, \frac{\chi_4}{\varepsilon} \right| \frac{1 + \lambda}{\varepsilon} \right)^2 - \frac{\phi(\lambda)}{q}, \]
where \( \chi_4 \) is a character of order 4 on \( \mathbb{F}_q \).

**Proof.** Putting \( \ell = 2 \) in Theorem 4.3.2 and then squaring both sides, we have
\[ a_q(V_{2, \lambda})^2 = q^2 \cdot \frac{J(\phi, \phi)^2}{J(\chi_4, \chi_4)^2} \cdot _2F_1 \left( \left. \frac{\chi_4}{\varepsilon}, \frac{\chi_4}{\varepsilon} \right| \frac{1 + \lambda}{\varepsilon} \right)^2. \]
By (1.3.2), we have \( J(\phi, \phi) = J(\chi_4, \chi_4) \). Hence comparing with (4.3.11), we complete the proof.

**Corollary 4.3.5.** Let \( q = p^e, p > 0 \) a prime and \( q \equiv 1 \pmod{4} \). If \( \alpha \beta \neq 0 \) and \( \alpha \neq \pm 2 \) such that \( \text{ord}_p(\frac{4(4-\alpha^2)}{\alpha^4}) = 0 \), then
\[ _2F_1 \left( \phi, \phi \left| \frac{\alpha - 2}{\alpha + 2} \right. \right)^2 = \phi(4 - \alpha^2) _3F_2 \left( \left. \phi, \phi, \phi \right| \frac{4}{4 - \alpha^2} \right) + \frac{1}{q}. \]
Proof. Replacing $\lambda$ by $\frac{4-\alpha^2}{\alpha^2}$ in Corollary 4.3.4, we have

$$2F_1\left(\frac{\chi_4}{\varepsilon}, \frac{\chi^4}{\varepsilon} \left| \frac{4}{\alpha^2}\right) = \phi(4-\alpha^2)3F_2\left(\frac{\phi}{\varepsilon}, \frac{\phi}{\varepsilon} \left| \frac{4}{4-\alpha^2}\right) + \frac{1}{q}.$$

Again, from Corollary 2.3.3, we obtain

$$2F_1\left(\frac{\chi_4}{\varepsilon}, \frac{\chi^4}{\varepsilon} \left| \frac{4}{\alpha^2}\right) = 2F_1\left(\frac{\phi}{\varepsilon}, \frac{\phi}{\varepsilon} \left| \frac{\alpha-2}{\alpha+2}\right).$$

Hence the proof follows. \qed

4.4 On $y^\ell = (x-1)(x^2 + \lambda)$ for $\lambda = \frac{1}{3}$

We now will consider the special case when $\lambda = \frac{1}{3}$ for the algebraic curve $V_{\ell,\lambda}$. In this case, simpler expressions for the Gaussian hypergeometric functions involved in Theorem 4.3.2 are known. We use a known transformation of the hypergeometric series in terms of the gamma function to simplify the expression as a binomial coefficient.

Theorem 4.4.1. If $q \equiv 1 \pmod{\ell}$, then for $\lambda = \frac{1}{3}$, we have

$$-a_q(V_{\ell,\lambda}) = \begin{cases} 0, & \text{if } \ell \neq 3 \text{ and } q \equiv 2 \pmod{3}; \\ q \cdot \sum_{i=1}^{\ell-1} S_i \left(\frac{27}{8}\right) \left[\left(\frac{\chi_3^{S_i}}{\chi_3^{S_i}}\right) + \left(\frac{\chi_3^{2S_i}}{\chi_3^{2S_i}}\right)\right], & \text{if } \ell \neq 3 \text{ and } q \equiv 1 \pmod{3}; \\ 2 + q \cdot \sum_{i=1}^{2} \left[\left(\frac{\chi_3^{S_i}}{\chi_3^{S_i}}\right) + \left(\frac{\chi_3^{2S_i}}{\chi_3^{2S_i}}\right)\right], & \text{if } \ell = 3, \end{cases}$$

where $S$ and $\chi_3$ are characters on $\mathbb{F}_q$ of order $\ell$ and 3 respectively.

Proof. Putting $\lambda = \frac{1}{3}$ in (4.3.1) and making the change of variables $(x, y) \to (\frac{x}{9} + \frac{1}{3}, y)$, and then replacing $-\frac{x}{9}$ by $x$ we obtain the equivalent equation of

$$y^\ell = (x-1)(x^2 + \lambda)$$
as
\[ y^\ell = -\frac{8}{27} (1 + x^3). \]

Therefore,
\[
\#\{(x, y) \in \mathbb{F}_q^2 : y^\ell = (x - 1)(x^2 + \frac{1}{3})\}
= \#\{(x, y) \in \mathbb{F}_q^2 : y^\ell = -\frac{8}{27} (1 + x^3)\}
= \sum_{x \in \mathbb{F}_q, 1 + x^3 \neq 0} \#\{y \in \mathbb{F}_q : y^\ell = -\frac{8}{27} (1 + x^3)\} + \#\{x \in \mathbb{F}_q : 1 + x^3 = 0\}
\]

Applying Lemma 1.3.6, we obtain
\[
\#\{(x, y) \in \mathbb{F}_q^2 : y^\ell = (x - 1)(x^2 + \frac{1}{3})\} = q + \sum_{i=1}^{\ell-1} \sum_{x \in \mathbb{F}_q} S_i \left( -\frac{8}{27} \right) S_i (1 + x^3).
\]

Now recall that the binomial theorem (see [18]) for a character \( A \) on \( \mathbb{F}_q \) is given by
\[
A(1 + x) = \delta(x) + \frac{q}{q-1} \sum_x \left( A \chi \right) \chi(x),
\]
where \( \delta(x) = 1 \) (resp. 0) if \( x = 0 \) (resp. \( x \neq 0 \)). Hence
\[
\#\{(x, y) \in \mathbb{F}_q^2 : y^\ell = (x - 1)(x^2 + \frac{1}{3})\}
= q + \sum_{i=1}^{\ell-1} \sum_{x \in \mathbb{F}_q} S_i \left( -\frac{8}{27} \right) \left[ \delta(x^3) + \frac{q}{q-1} \sum_x \left( S^i \chi \right) \chi(x^3) \right]
= q + \sum_{i=1}^{\ell-1} S_i \left( -\frac{8}{27} \right) + \frac{q}{q-1} \sum_{i=0}^{\ell-1} S_i \left( -\frac{8}{27} \right) \sum_x \left( S_i \chi \right) \sum_x x^3(x). \tag{4.4.1}
\]

By Lemma 1.3.7, \( \sum_{x \in \mathbb{F}_q} x^3(x) \) is nonzero if and only if \( \chi^3 = \varepsilon \), which is possible only for \( \varepsilon, \chi_3 \) and \( \chi_3^2 \). Therefore, (4.4.1) reduces to
\[
\#\{(x, y) \in \mathbb{F}_q^2 : y^\ell = (x - 1)(x^2 + \frac{1}{3})\}
= \begin{cases} 
q, & \text{if } q \equiv 2 \pmod{3}; \\
q + q \cdot \sum_{i=1}^{\ell-1} S_i \left( \frac{27}{8} \right) \left[ \left( \chi_3 \right) + \left( \chi_3^2 \right) \right], & \text{if } q \equiv 1 \pmod{3},
\end{cases}
\]
which completes the proof of the result because of (4.3.3) and (4.3.4). \( \square \)
We now give an alternate proof of a result of McCarthy [30]. In this result, the trace of Frobenius of an elliptic curve is expressed in terms of the binomial coefficient of characters, which can be also express in terms of Gauss sums.

**Theorem 4.4.2.** [30, Thm. 2.3] If \( q \equiv 1 \pmod{3} \), then

\[
-\frac{\phi(-2)}{q} \cdot a_q(V_{2,\frac{1}{3}}) = 2\text{Re}\left(\chi_3\right)
\]

and

\[
-\phi(-2) \cdot a_q(V_{2,\frac{1}{3}}) = 2\text{Re}\left[\frac{G(\chi_3)G(\phi)}{G(\chi_3\phi)}\right],
\]

where \( \chi_3 \) is a character of order 3 on \( \mathbb{F}_q \) and \( G(\chi) \) is a Gauss sum.

**Proof.** Since \( q \equiv 1 \pmod{3} \), putting \( \ell = 2 \) in Theorem 4.4.1 we find that

\[
-a_q(V_{2,\frac{1}{3}}) = q\phi(6) \left[ \left(\chi_3\right) + \left(\chi_3^2\right) \right].
\]

We know that \( \phi(-3) = 1 \) if and only if \( q \equiv 1 \pmod{3} \). Hence the first part of the theorem follows from the fact that \( \left(\chi_3\right)^{q-1} = \left(\chi_3^2\right)^{q-1} \).

Again the second part follows from the fact that if \( \chi\psi \) is nontrivial, then

\[
\left(\chi,\psi\right) = \frac{\psi(-1)}{q} J(\chi,\psi) = \frac{\psi(-1)}{q} G(\chi)G(\psi),
\]

where \( J(\chi,\psi) \) and \( G(\chi) \) are Jacobi and Gauss sums respectively.

Simplifying the expression for \( a_q(V_{\ell,\lambda}) \) given in Theorem 4.4.1, we obtain the following result which generalizes the case \( \ell = 2 \), treated in Theorem 4.4.2.

**Corollary 4.4.3.** Let \( d = \text{lcm}(3,\ell) \). If \( q \equiv 1 \pmod{d} \), then

\[
-a_q(V_{\ell,\frac{1}{3}}) = \begin{cases} 
2 + 2q \cdot \text{Re} \left[ \left(\chi_3\right) + \left(\chi_3^2\right) \right], & \text{if } \ell = 3; \\
2q \cdot \sum_{i=1}^{\frac{\ell-1}{2}} \text{Re} \left[ S^i \left(\frac{27}{8}\right) \left(\chi_3\right) + \left(\chi_3^2\right) \right], & \text{if } \ell \text{ is odd}, \ell > 3; \\
2q \cdot \phi(-2)\text{Re} \left(\chi_3\right) + \sum_{i=1}^{\frac{\ell-2}{2}} \text{Re} \left( S^i \left(\frac{27}{8}\right) \left(\chi_3\right) + \left(\chi_3^2\right) \right), & \text{if } \ell \text{ is even};
\end{cases}
\]

where \( S \) and \( \chi_3 \) are characters on \( \mathbb{F}_q \) of order \( \ell \) and 3 respectively.
Proof. Applying the same procedure as followed in the proof of Corollary 3.3.3 in the expression of Theorem 4.4.1, we can obtain the result.