

CENTRAL LIBRARY  
TEZPUR UNIVERSITY

Accession No. T 273

Date 23/5/14

THESES & DISSERTATION  
SECTION  
CENTRAL LIBRARY, T.U.

# CERTAIN FAMILIES OF ALGEBRAIC CURVES AND POLYNOMIALS, AND THEIR CONNECTIONS TO HYPERGEOMETRIC FUNCTIONS

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE  
REQUIREMENTS FOR THE DEGREE OF  
DOCTOR OF PHILOSOPHY  
IN  
MATHEMATICAL SCIENCES

By  
Gautam Kalita

Registration No. TZ121461 of 2012



DEPARTMENT OF MATHEMATICAL SCIENCES  
SCHOOL OF SCIENCES  
TEZPUR UNIVERSITY, NAPAAM-784028  
ASSAM, INDIA

NOVEMBER 2013

**Dedicated to my parents  
and  
supervisor**

# Abstract

The central theme of our work is to explore connections between values of hypergeometric functions and algebraic curves. The theory of classical hypergeometric series has been studied for centuries and their associations with counting points on algebraic curves have been fully explored. In 1980's, Greene introduced the notion of hypergeometric functions over finite fields analogous to classical hypergeometric series. Since then, connections between number of points on elliptic curves and hypergeometric functions over finite fields have been investigated by many mathematicians such as Ahlgren, Frechette, Koike, Ono, and Papanikolas.

Recently, Fuselier gave formulas for traces of Frobenius of certain families of elliptic curves in terms of Gaussian hypergeometric functions involving characters of orders 12 as parameters for primes  $p$  satisfying  $p \equiv 1 \pmod{12}$ . Following her approach, Lennon provided a general formula for the number of  $\mathbb{F}_q$ -points of an elliptic curve  $E$  with  $j(E) \neq 0, 1728$  in terms of values of Gaussian hypergeometric series containing characters of order 12 for  $q = p^e \equiv 1 \pmod{12}$ . Following these, in this dissertation, we present some general formulas connecting the number of points on certain families of elliptic curves given by Weierstrass normal form over  $\mathbb{F}_q$  with Gaussian hypergeometric series containing characters of order 6, 4, and 3, separately.

Most recently, Vega considered certain more general families of algebraic curves and expressed the number of  $\mathbb{F}_q$ -points on those families as a linear combination of  ${}_2F_1$  hypergeometric functions. In our work, we have considered two families of algebraic curves, namely  $y^\ell = x(x-1)(x-\lambda)$  and  $y^\ell = (x-1)(x^2 + \lambda)$ ; and give

explicit formulas for the number of  $\mathbb{F}_q$ -points on these families as sums of values of  ${}_2F_1$  and  ${}_3F_2$  Gaussian hypergeometric series, respectively. These formulas generalize certain known results on elliptic curves and Gaussian hypergeometric series. Further, we define period analogue for the algebraic curve  $y^\ell = x(x-1)(x-\lambda)$ , and obtain an expression for the period analogue in terms of  ${}_2F_1$  classical hypergeometric series.

In all the known results connecting Gaussian hypergeometric series and algebraic curves, expressions are obtained in terms of  ${}_2F_1$  and  ${}_3F_2$  Gaussian hypergeometric series. Hence, the task remained to find similar results for  ${}_{n+1}F_n$  Gaussian hypergeometric series for  $n \geq 3$ . Ahlgren and Ono studied this problem and deduced the value of  ${}_4F_3$  hypergeometric series at 1 over  $\mathbb{F}_p$  in terms of representations of  $4p$  as a sum of four squares using the fact that the Calabi-Yau threefold is modular. For  $n > 3$ , the non-trivial values of  ${}_{n+1}F_n$  Gaussian hypergeometric series are difficult to obtain, and this problem was also mentioned by Ono. We present explicitly the number of distinct zeros of the polynomial  $x^d + ax + b$  over  $\mathbb{F}_q$  in terms of the Gaussian hypergeometric functions  ${}_dF_{d-1}$  and  ${}_{d-1}F_{d-2}$  containing characters of orders  $d$  and  $d-1$  as parameters.

Finally, we deduce certain special values of  ${}_2F_1$  and  ${}_3F_2$  Gaussian hypergeometric series containing higher order characters as parameters using our results.

## DECLARATION BY THE CANDIDATE

I, Gautam Kalita, hereby declare that the subject matter in this thesis entitled “**Certain families of algebraic curves and polynomials, and their connections to hypergeometric functions**”, is the record of work done by me, that the contents of this thesis did not form basis of the award of any previous degree to me or to the best of my knowledge to anybody else, and that the thesis has not been submitted by me for any research degree in any other university/institute.

This thesis is being submitted to the Tezpur University for the degree of Doctor of Philosophy in Mathematical Sciences.

Place: Tezpur.

Date: 25/10/2013

*Gautam Kalita*  
**Signature of the candidate**



## TEZPUR UNIVERSITY

---

### CERTIFICATE OF THE SUPERVISORS

This is to certify that the thesis entitled **Certain families of algebraic curves and polynomials, and their connections to hypergeometric functions** submitted to the School of Sciences of Tezpur University in partial fulfillment for the award of the degree of Doctor of Philosophy in Mathematical Sciences is a record of research work carried out by **Mr. Gautam Kalita** (Registration No. TZ121461 of 2012) under my supervision and guidance.

All help received by him from various sources have been duly acknowledged.

No part of this thesis have been submitted elsewhere for award of any other degree.

Signature of Supervisor

**Dr. Rupam Barman**<sup>1</sup>

School of Sciences

Department of Mathematical Sciences

Tezpur University

Assam, India.

Signature of Co-supervisor

**Prof. Nayandeep Deka Baruah**

School of Sciences

Department of Mathematical Sciences

Tezpur University

Assam, India.

---

<sup>1</sup>Current Address: Department of Mathematics, IIT Delhi, Hauz Khas, New Delhi, India.

# Acknowledgements

First and foremost, I offer my sincere gratitude to my supervisor Dr. Rupam Barman for his foresight, invaluable suggestions, continuous encouragement and for being an infinite source of inspiration and motivation. I am proud to be the first in what is sure to be a long line of your students.

I am thankful to my co-supervisor Prof. Nayandeep Deka Baruah for his cooperation, suggestions, and fruitful discussions.

I would like to thank Prof. Ken Ono for his continuous support, inspiration, and suggestions. I am really grateful to him for clarifying all my queries from the early stage of my PhD without which this work would not be possible. Thanks to Prof. Dipendra Prasad and Prof. R. Sujatha for their support during my PhD period.

I am indeed grateful to all the faculty members of the Department of Mathematical Sciences, Tezpur University for their valuable suggestions and advice. Special thanks to Dr. Rajib Haloi for his continuous support during my PhD years.

I gratefully acknowledge the financial support received from the Department of Science and Technology, Government of India through INSPIRE fellowship.

It is my privilege to thank all family members of Dr. Rupam Barman for their hospitality at Guwahati during the time of my visit for research works.

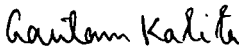
I thank all my fellow research scholars for helping me in many ways and making my stay enjoyable at TU during these years. Special thanks to Jayanta for all his helps. I also thank my colleagues at DBCET for their help and cooperations.

I am indebted to my uncle Mr. Prasanta Kalita for making mathematics interesting for me from my childhood and inspire me throughout.

Finally, I appreciate all of the love, blessings from my parents, bhaiti, bhanti, and Sona. I thank them for their continuous support and never ending faith in me.

Date: 25/10/2013

Place: Tezpur

  
(Gautam Kalita)



# Table of Contents

<b>Abstract</b>	<b>iii</b>
<b>Acknowledgements</b>	<b>vii</b>
<b>Table of Contents</b>	<b>viii</b>
<b>1 Introduction</b>	<b>1</b>
1.1 General introduction . . . . .	1
1.2 Brief history . . . . .	2
1.2.1 Classical hypergeometric series and elliptic curves . . . . .	2
1.2.2 Gaussian hypergeometric function and algebraic curves . . . . .	4
1.3 Preliminaries . . . . .	8
1.3.1 Classical hypergeometric series . . . . .	8
1.3.2 Characters on finite fields . . . . .	10
1.3.3 Gaussian hypergeometric functions . . . . .	12
1.4 Organization . . . . .	15
<b>2 Elliptic Curves and Gaussian Hypergeometric Series</b>	<b>16</b>
2.1 Introduction . . . . .	16
2.2 Traces of Frobenius endomorphism of elliptic curves . . . . .	17
2.2.1 Case 1: $q \equiv 1 \pmod{6}$ . . . . .	18
2.2.2 Case 2: $q \equiv 1 \pmod{4}$ . . . . .	23
2.2.3 Case 3: $q \equiv 1 \pmod{3}$ . . . . .	26
2.3 Number of $\mathbb{F}_q$ -points on Edward form of elliptic curve . . . . .	30

<b>3</b>	<b>Hypergeometric Functions and <math>y^\ell = x(x-1)(x-\lambda)</math></b>	<b>36</b>
3.1	Introduction . . . . .	36
3.2	Main results . . . . .	37
3.2.1	On $y^\ell = x(x-1)(x-\lambda)$ and classical hypergeometric series .	37
3.2.2	On $y^\ell = x(x-1)(x-\lambda)$ and Gaussian hypergeometric function	39
3.3	Analog between classical and Gaussian hypergeometric series . . . . .	43
<b>4</b>	<b>Gaussian Hypergeometric Series and <math>y^\ell = (x-1)(x^2+\lambda)</math></b>	<b>49</b>
4.1	Introduction . . . . .	49
4.2	Preliminaries . . . . .	50
4.3	Main results . . . . .	52
4.3.1	$y^\ell = (x-1)(x^2+\lambda)$ and ${}_3F_2$ Gaussian hypergeometric series .	54
4.3.2	$y^\ell = (x-1)(x^2+\lambda)$ and ${}_2F_1$ Gaussian hypergeometric series .	57
4.4	On $y^\ell = (x-1)(x^2+\lambda)$ for $\lambda = \frac{1}{3}$ . . . . .	61
<b>5</b>	<b>On The Polynomial <math>x^d+ax+b</math> and Gaussian Hypergeometric Series</b>	<b>65</b>
5.1	Introduction . . . . .	65
5.2	Main results . . . . .	66
5.2.1	Number of zeros of $x^d+ax+b$ for even $d$ . . . . .	67
5.2.2	Number of zeros of $x^d+ax+b$ for odd $d$ . . . . .	71
<b>6</b>	<b>Special Values of Gaussian Hypergeometric Series</b>	<b>75</b>
6.1	Introduction . . . . .	75
6.2	Main results . . . . .	76
6.2.1	Values of ${}_2F_1$ Gaussian hypergeometric series . . . . .	76
6.2.2	Values of ${}_3F_2$ Gaussian hypergeometric series . . . . .	82
	<b>Bibliography</b>	<b>86</b>
	<b>Publications</b>	<b>90</b>

# Chapter 1

## Introduction

### 1.1 General introduction

The problem of finding the number of solutions of a polynomial equation over a field, in particular, over a finite field, has been of interest to mathematicians for many years. Recently, lots of progress have been made in this direction which paves the way to solve many important congruences, old conjectures, and related problems. Mathematicians such as Ahlgren, Fuselier, Frechette, Koike, Ono, and Papanikolas have found many interesting connections of different parameters of algebraic curves and modular forms with hypergeometric functions over finite fields. For example, explicit formulas for traces of Frobenius of elliptic curves and traces of Hecke operators on certain spaces of modular forms are obtained in terms of Gaussian hypergeometric series. For details, see [2, 3, 14, 15, 16, 27, 28].

An algebraic curve or affine curve  $E$  over a field  $K$  is defined as the set of all points satisfying a polynomial equation in two variables  $P(x, y) = 0$  over  $K$ . It is easy to check that if both the partial derivatives  $\frac{\partial P}{\partial x}$  and  $\frac{\partial P}{\partial y}$  do not vanish simultaneously at any point on  $E$ , there is a well-defined tangent line at every point on  $E$ . Such a curve is called a non-singular curve, otherwise it is singular. The projective form  $C$  of an algebraic curve  $E$  defined by  $P(x, y)$  is the collection of all points which satisfy the homogenous polynomial equation  $P(x, y, z) = 0$  in three variables. If  $z \neq 0$ , there is always a one-to-one correspondence between the points on  $E$  and the points on  $C$ . For  $z = 0$ , the points on  $C$  are called the points at infinity of  $E$ . For

details, see [24].

In 1812, Gauss presented to the Royal Society of Sciences at Göttingen his famous paper [17] in which he defined  ${}_2F_1$  classical hypergeometric series. He also gave criteria for the convergence of such infinite series in the same paper. Since then, connections between classical hypergeometric series and different mathematical objects have been investigated by mathematicians. Meanwhile, in 1980's, Greene introduced finite field analog of classical hypergeometric series as finite character sums called Gaussian hypergeometric function. It is found that this function also has many interesting connections with algebraic curves, modular forms, and other mathematical objects in the same way as classical hypergeometric series do.

In this chapter, we begin by giving a survey of recent works in which classical hypergeometric series and Gaussian hypergeometric series are connected with different parameters of algebraic curves, in particular elliptic curves. We recall definitions of classical hypergeometric series, characters on finite fields, and Gaussian hypergeometric functions and list a few of their properties.

## 1.2 Brief history

### 1.2.1 Classical hypergeometric series and elliptic curves

The Classical hypergeometric series have been studied for centuries. Ramanujan had studied classical hypergeometric series more extensively and contributed a lot in this area. He found many connections of classical hypergeometric series with other number theoretical functions.

For a complex number  $a$  and a non-negative integer  $n$ , let  $(a)_n$  denote the rising factorial defined by

$$(a)_0 := 1 \quad \text{and} \quad (a)_n := a(a+1)(a+2) \cdots (a+n-1) \quad \text{for} \quad n > 0.$$

Then, for complex numbers  $a_i, b_j$  and  $z$ , with none of the  $b_j$  being negative integers

or zero, the classical hypergeometric series is defined as

$${}_{r+1}F_r \left( \begin{matrix} a_0, & a_1, & \dots, & a_r \\ & b_1, & \dots, & b_r \end{matrix} \mid z \right) := \sum_{n=0}^{\infty} \frac{(a_0)_n (a_1)_n \cdots (a_r)_n z^n}{(b_1)_n (b_2)_n \cdots (b_r)_n n!}.$$

This hypergeometric series converges absolutely for  $|z| < 1$ . The series also converges absolutely for  $|z| = 1$  if  $\operatorname{Re}(\sum b_i - \sum a_i) > 0$  and converges conditionally for  $|z| = 1, z \neq 1$  if  $0 \geq \operatorname{Re}(\sum b_i - \sum a_i) > -1$ . For details, see [4, 5]. Classical hypergeometric series satisfy many interesting symmetries and transformation identities [38].

The relations of classical hypergeometric series with different mathematical objects, for example, number of points on algebraic curves have been investigated by many mathematicians. In 1836, Kummer found a striking connection between the real period of a family of elliptic curves and classical hypergeometric series as given in the following theorem.

**Theorem 1.2.1.** [22, Thm. 6.1] *If  $0 < t < 1$ , then the real period  $\Omega({}_2E_1)$  of the elliptic curve*

$${}_2E_1(t) : y^2 = x(x-1)(x-t),$$

*is given by*

$$\frac{\Omega({}_2E_1)}{\pi} = {}_2F_1 \left( \begin{matrix} \frac{1}{2}, & \frac{1}{2} \\ & 1 \end{matrix} \mid t \right).$$

At the beginning of 20th century, mathematicians such as Beukers, Stiller, and others studied about classical hypergeometric series more extensively, and investigated relations of this series with modular forms and other mathematical objects. In [39], Stiller connected classical hypergeometric series with graded algebra generated by classical Eisenstein series  $E_4$  and  $E_6$ . Soon after, Beukers [8] represented a period of the lattice associated to the family of elliptic curves  ${}_2E'_1(t) : y^2 = x^3 - x - t$  as a constant multiple of  ${}_2F_1$  classical hypergeometric series. In fact, he identified the period  $\Omega({}_2E'_1)$  of the elliptic curve  ${}_2E'_1$  as a constant multiple of  ${}_2F_1 \left( \begin{matrix} \frac{1}{12}, & \frac{5}{12} \\ & \frac{1}{2} \end{matrix} \mid \frac{27}{4}t^2 \right)$ .

Recently, McCarthy [30] considered the Clausen family of elliptic curve and gave a relation between a period of the elliptic curve and  ${}_3F_2$  hypergeometric series.

**Theorem 1.2.2.** [30, Thm. 2.1] *Let  ${}_3E_2$  be the elliptic curve defined by*

$${}_3E_2(t) : y^2 = (x-1)(x^2+t), \quad t \in \mathbb{Q} \setminus \{0, -1\}.$$

*Then for  $t > 0$ ,*

$${}_3F_2 \left( \begin{matrix} \frac{1}{2}, & \frac{1}{2}, & \frac{1}{2} \\ 1, & 1 \end{matrix} \middle| \frac{t}{1+t} \right) = \frac{\sqrt{1+t} \Omega({}_3E_2)^2}{\pi^2},$$

*where  $\Omega({}_3E_2)$  is the real period of  ${}_3E_2(t)$ .*

It is to be noted that the Clausen family of elliptic curve  ${}_3E_2$  has only one real point of order 2 for  $t > 0$ ; whereas the Legendre's family of elliptic curve  ${}_2E_1$  considered by Kummer has three real points of order 2.

## 1.2.2 Gaussian hypergeometric function and algebraic curves

Analogous to the classical hypergeometric series, Greene [18] introduced hypergeometric series over finite fields or Gaussian hypergeometric series. Let  $\mathbb{F}_q$  denote the finite field with  $q$  elements, where  $q = p^e$ ,  $p$  is a prime and  $e \in \mathbb{N}$ . Extend each multiplicative character  $\chi : \mathbb{F}_q^\times \rightarrow \mathbb{C}^\times$  to  $\mathbb{F}_q$  by defining  $\chi(0) = 0$ . For characters  $A$  and  $B$  of  $\mathbb{F}_q$ , the binomial coefficient  $\binom{A}{B}$  is defined by

$$\binom{A}{B} := \frac{B(-1)}{q} J(A, \bar{B}) = \frac{B(-1)}{q} \sum_{x \in \mathbb{F}_q} A(x) \bar{B}(1-x),$$

where  $J(A, B)$  denotes the usual Jacobi sum and  $\bar{B}$  is the inverse of  $B$ . With this notation, for characters  $A_0, A_1, \dots, A_n$  and  $B_1, B_2, \dots, B_n$  of  $\mathbb{F}_q$ , the Gaussian hypergeometric series over  $\mathbb{F}_q$  is defined as

$${}_{n+1}F_n \left( \begin{matrix} A_0, & A_1, & \dots, & A_n \\ & B_1, & \dots, & B_n \end{matrix} \middle| x \right) := \frac{q}{q-1} \sum_{\chi} \binom{A_0\chi}{\chi} \binom{A_1\chi}{B_1\chi} \cdots \binom{A_n\chi}{B_n\chi} \chi(x),$$

where the sum is over all characters  $\chi$  of  $\mathbb{F}_q$ .

Greene explored properties of these functions and found that they satisfy many summation and transformation formulas analogous to classical hypergeometric series. These similarities generated interest in finding connections that hypergeometric functions over finite fields may have with other objects, for example elliptic curves and modular forms.

Define an elliptic curve  $E$  over  $\mathbb{Q}$  in Weierstrass form by

$$E : y^2 = x^3 + ax + b.$$

The discriminant  $\Delta(E)$  and  $j$ -invariant  $j(E)$  of  $E$  are given by

$$\Delta(E) = -16(4a^3 + 27b^2), \quad \text{and} \quad j(E) = \frac{(-48a)^3}{\Delta(E)} = \frac{2^8 3^3 a^3}{4a^3 + 27b^2}.$$

For a prime  $p$  of good reduction, that is, if  $p \nmid \Delta(E)$ , the trace of Frobenius for  $E$  is given by

$$a_p(E) = 1 + p - \#E(\mathbb{F}_p),$$

where

$$E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p^2 : y^2 = x^3 + ax + b\} \cup \{P\}$$

denotes the set of points on  $E$  over  $\mathbb{F}_p$  together with the point at infinity  $P = [0 : 1 : 0]$ . Again, if  $p \mid \Delta(E)$ , that is,  $p$  is a bad prime, then  $a_p(E) = 0, \pm 1$  depending on the nature of singularity.

The Hasse-Weil  $L$ -function associated to an elliptic curve  $E$  is defined in terms of traces of Frobenius of the elliptic curve by the Euler product

$$L(E, s) := \prod_{p \mid \Delta(E)} (1 - a_p p^{-s})^{-1} \prod_{p \nmid \Delta(E)} (1 - a_p p^{-s} + p^{1-2s})^{-1},$$

where  $s$  is a complex number with  $\text{Re}(s) > \frac{3}{2}$ . Further, the  $L$ -function has close connection with the rank of the elliptic curve as conjectured by Birch, Swinnerton, and Dyer. Thus, the trace of Frobenius of an elliptic curve  $E$  is an interesting parameter, and finding simple expressions for  $a_p(E)$  in terms of different mathematical objects is a problem of interest.

Consider the following two families of elliptic curves defined by

$${}_2E_1 : y^2 = x(x-1)(x-t), \quad t \neq 0, 1$$

$${}_3E_2 : y^2 = (x-1)(x^2+t), \quad t \neq 0, -1.$$

In the following theorem, Koike [25] and Ono [34] gave explicit formulas for the traces of Frobenius of the above families of elliptic curves in terms of Gaussian hypergeometric series.

**Theorem 1.2.3.** ((a) [25], (b) [34]) Let  $p$  be an odd prime. Then

$$(a) \quad p \cdot {}_2F_1 \left( \begin{matrix} \phi, & \phi \\ & \varepsilon \end{matrix} \mid t \right) = -\phi(-1)a_p({}_2E_1)$$

$$(b) \quad p^2 \cdot {}_3F_2 \left( \begin{matrix} \phi, & \phi, & \phi \\ \varepsilon, & \varepsilon \end{matrix} \mid 1 + \frac{1}{t} \right) = \phi(-t)(a_p({}_3E_2)^2 - p),$$

where  $\phi$  and  $\varepsilon$  are quadratic and trivial characters on  $\mathbb{F}_p$ , respectively.

These results are analogous to the expressions of real periods of the same families of elliptic curves in terms of classical hypergeometric series stated in Theorem 1.2.1 and Theorem 1.2.2. In these formulas, only quadratic and trivial characters are used as parameter, and thus the task remained to find expressions with higher order characters as parameters [35]. Following are some of the directions where the relations of Gaussian hypergeometric series containing higher order characters and number of  $\mathbb{F}_q$ -points on families of varieties have been explored.

In [14], Fuselier gave formulas for the trace of Frobenius of certain families of elliptic curves which involved Gaussian hypergeometric series with characters of order 12 as parameters, under the assumption that  $p \equiv 1 \pmod{12}$ .

**Theorem 1.2.4.** [14, Thm. 1.2] *Suppose  $p$  is a prime,  $p \equiv 1 \pmod{12}$  and  $\xi \in \widehat{\mathbb{F}_p^\times}$  has order 12. If  $t \in \mathbb{F}_p \setminus \{0, 1\}$ , then for the elliptic curve*

$$E_t : y^2 = 4x^3 - \frac{27}{1-t}x - \frac{27}{1-t}$$

with  $j(E_t) = \frac{1728}{t}$ , we have

$$p \cdot {}_2F_1 \left( \begin{matrix} \xi, & \xi^5 \\ & \varepsilon \end{matrix} \mid t \right) = \frac{-\phi(2)}{\xi^3(1-t)}a_p(E_t).$$

In the same paper, Fuselier also considered elliptic curves constructed by Beukers [8], and found a striking resemblance between the Gaussian hypergeometric function expression of the trace of Frobenius and classical hypergeometric series expression of a period of the same family of elliptic curves.

Afterwards, for  $q \equiv 1 \pmod{3}$ , Lennon gave formulas for certain elliptic curves involving Gaussian hypergeometric series with characters of order 3 as parameters in [28].



**Theorem 1.2.5.** [28, Thm. 1.1] *Let  $E_{a_1, a_3}$  be an elliptic curve over  $\mathbb{Q}$  in the form given by the equation*

$$E_{a_1, a_3} : y^2 + a_1xy + a_3y = x^3 .$$

*and let  $p$  be a prime for which  $E_{a_1, a_3}$  has good reduction. Also assume that  $p \nmid a_1$ , and  $q = p^e \equiv 1 \pmod{3}$ . Let  $\rho \in \widehat{\mathbb{F}_q^\times}$  be a character of order three, and let  $\varepsilon$  be the trivial character. If  $\tilde{E}_{a_1, a_3}$  denotes the curve obtained by reduced modulo  $p$  of  $E_{a_1, a_3}$ , then the trace of the Frobenius map on  $\tilde{E}_{a_1, a_3}$  is given by*

$$a_q(\tilde{E}_{a_1, a_3}) = -q \cdot {}_2F_1 \left( \rho, \rho^2 \mid \frac{27a_3}{a_1^3} \right).$$

In all of the above results, the character parameters in the hypergeometric series depended on the family of curves considered. In addition, the values at which the hypergeometric series are evaluated are functions of the coefficients and so depended on the model used. Lennon [27] gave a general formula expressing the number of  $\mathbb{F}_p$ -points of an elliptic curve in terms of more intrinsic properties of the curve without having to put the curve in a specific form. Consecutively, Lennon removed the restriction on  $p$  imposed by Fuselier [14], and provided a general formula connecting the number of  $\mathbb{F}_q$ -points on an elliptic curve  $E$  with  $j(E) \neq 0, 1728$  with Gaussian hypergeometric series for  $q = p^e \equiv 1 \pmod{12}$ .

**Theorem 1.2.6.** [27, Thm. 1.1] *Let  $q = p^e, p > 0$  a prime and  $q \equiv 1 \pmod{12}$ . In addition, let  $E$  be an elliptic curve over  $\mathbb{F}_q$  with  $j(E) \neq 0, 1728$  and  $T \in \widehat{\mathbb{F}_q^\times}$  a generator of the character group. The trace of the Frobenius map on  $E$  can be expressed as*

$$a_q(E) = -q \cdot T^{\frac{q-1}{12}} \left( \frac{1728}{\Delta(E)} \right) \cdot {}_2F_1 \left( T^{\frac{q-1}{12}}, T^{\frac{q-1}{12}} \mid \frac{j(E)}{1728} \right),$$

where  $\Delta(E)$  is the discriminant of  $E$ .

All formulas stated above connect Gaussian hypergeometric series with number of  $\mathbb{F}_q$ -points on elliptic curves. Therefore, a natural question to ask is whether there are similar formulas for counting points of more general curves in terms of Gaussian hypergeometric series. Most recently, Vega in [40], generalized this problem to more general curves of degree  $\ell > 0$ . For  $z \in \mathbb{F}_q$ , Vega considered the smooth projective curve with affine equation given by

$$C_z : y^\ell = x^m(1-x)^s(1-zx)^m,$$

where  $\ell \in \mathbb{N}$  and  $1 \leq m, s < \ell$  such that  $m + s = \ell$ . She explicitly related the number of points on  $C_z$  over  $\mathbb{F}_q$  with Gaussian hypergeometric functions containing characters of order  $\ell$  as parameters.

**Theorem 1.2.7.** [40, Thm. 1.1] *Let  $a = \frac{m}{n}$  and  $b = \frac{s}{r}$  be rational numbers such that  $0 < a, b < 1$ , and let  $z \in \mathbb{F}_q$ ,  $z \neq 0, 1$ . Consider the smooth projective algebraic curve with affine equation given by*

$$C_z^{(a,b)} : y^\ell = x^{\ell(1-b)}(1-x)^{\ell b}(1-zx)^{\ell a},$$

where  $\ell = \text{lcm}(n, r)$ . If  $q \equiv 1 \pmod{\ell}$ , then

$$\#C_z^{(a,b)}(\mathbb{F}_q) = q + 1 + q \sum_{i=1}^{\ell-1} \chi^{i\ell b}(-1) {}_2F_1 \left( \begin{matrix} \chi^{i\ell(1-a)}, & \chi^{i\ell(1-b)} \\ \varepsilon & \end{matrix} \mid z \right),$$

where  $\chi \in \widehat{\mathbb{F}_q^\times}$  is a character of order  $\ell$  and  $\#C_z^{(a,b)}(\mathbb{F}_q)$  denotes the number of points that the curve  $C_z^{(a,b)}$  has over  $\mathbb{F}_q$ .

In the same paper, she proposed a conjecture connecting the  ${}_2F_1$  hypergeometric function of the above theorem and the reciprocal roots of zeta functions of  $C_z$ . She also proved the conjecture for some special cases.

## 1.3 Preliminaries

In this section, we define classical hypergeometric series, characters on finite fields, and Gaussian hypergeometric series. We list properties of characters and recall some symmetric and transformation identities of hypergeometric functions which will be used to prove our results. We start with the classical hypergeometric series.

### 1.3.1 Classical hypergeometric series

The classical hypergeometric series is an old example of infinite series. In 1810's, Gauss defined classical hypergeometric series in one of his famous papers. For  $a, b, c \in \mathbb{C}$ , he defined  ${}_2F_1$  classical hypergeometric series as

$${}_2F_1 \left( \begin{matrix} a, & b \\ & c \end{matrix} \mid z \right) = \frac{(a)_n (b)_n}{(c)_n} \cdot \frac{z^n}{n!}.$$

Mathematicians such as Euler, Kummer, and Vandermonde studied this series and found many interesting identities and transformation formulas. The classical hypergeometric series satisfy a beautiful integral representation due to Euler [10] given as

$${}_2F_1 \left( \begin{matrix} a, & b \\ & c \end{matrix} \middle| z \right) = \frac{2\Gamma(c)}{\Gamma(b)\Gamma(c-b)} \int_0^1 t^{b-1}(1-t)^{c-b-1}(1-zt)^{-a} dt,$$

where  $\operatorname{Re} c > \operatorname{Re} b > 0$ . Again, making a change of variables, the above integral can be stated as follows.

**Theorem 1.3.1.** [9, p. 115] For  $\operatorname{Re} c > \operatorname{Re} b > 0$ ,

$${}_2F_1 \left( \begin{matrix} a, & b \\ & c \end{matrix} \middle| z \right) = \frac{2\Gamma(c)}{\Gamma(b)\Gamma(c-b)} \int_0^{\pi/2} \frac{(\sin t)^{2b-1}(\cos t)^{2c-2b-1}}{(1-z\sin^2 t)^a} dt.$$

Kummer showed that  ${}_2F_1$  classical hypergeometric series satisfy a well known second order differential equation. The classical hypergeometric series enjoy many interesting symmetric and transformation properties. For example, the Pfaff's transformation is given as follows.

**Theorem 1.3.2.** [38, p. 31]

$${}_2F_1 \left( \begin{matrix} a, & b \\ & c \end{matrix} \middle| x \right) = (1-x)^{-a} {}_2F_1 \left( \begin{matrix} a, & c-b \\ & c \end{matrix} \middle| \frac{x}{x-1} \right).$$

Many special values of classical hypergeometric series have been evaluated by mathematicians such as Gauss, Kummer, Vandermonde and Pfaff. In [17], Gauss deduced the following special value of classical hypergeometric series.

**Theorem 1.3.3.** *If  $\operatorname{Re}(c-a-b) > 0$ , then*

$${}_2F_1 \left( \begin{matrix} a, & b \\ & c \end{matrix} \middle| 1 \right) = \frac{\Gamma(c)\Gamma(c-a-b)}{\Gamma(c-a)\Gamma(c-b)}.$$

Further, the Kummer's Theorem is given by

**Theorem 1.3.4.** [5, p. 9]

$${}_2F_1 \left( \begin{matrix} a, & b \\ & 1+b-a \end{matrix} \middle| -1 \right) = \frac{\Gamma(1+b-a)\Gamma(1+\frac{b}{2})}{\Gamma(1+b)\Gamma(1+\frac{b}{2}-a)}.$$

### 1.3.2 Characters on finite fields

Let  $\mathbb{F}_q$  be the finite field with  $q$  elements, where  $q = p^e$ ,  $p$  is prime and  $e$  is a positive integer. Recall that  $\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$  is a cyclic multiplicative group of order  $q - 1$ . A multiplicative character  $\chi : \mathbb{F}_q^\times \rightarrow \mathbb{C}^\times$  is a group homomorphism. Throughout, we reserve the notations  $\varepsilon$  and  $\phi$  for trivial and quadratic characters, respectively. Thus, for  $x \in \mathbb{F}_q^\times$

$$\varepsilon(x) = 1,$$

and

$$\phi(x) = \left(\frac{x}{q}\right) = \begin{cases} 1, & \text{if } x \text{ is square of some element in } \mathbb{F}_q^\times; \\ -1, & \text{if } x \text{ is not square of any element in } \mathbb{F}_q^\times, \end{cases}$$

is the Legendre symbol. The following theorem gives the structure of multiplicative characters on  $\mathbb{F}_q$ . Also, every multiplicative character on  $\mathbb{F}_q$  can be constructed from the following theorem.

**Theorem 1.3.5.** [29, Thm. 5.8, p. 192] *Let  $g$  be a generator of the multiplicative group of  $\mathbb{F}_q$ . For each  $j = 0, 1, 2, \dots, q - 2$ , the function*

$$\chi_j(g^k) = e^{\frac{2\pi i j k}{q-1}}, \quad \text{for } k = 0, 1, 2, \dots, q - 2,$$

*defines a multiplicative character on  $\mathbb{F}_q$ .*

The set  $\widehat{\mathbb{F}_q^\times}$  of all multiplicative characters on  $\mathbb{F}_q^\times$  is a cyclic group under multiplication of characters [6, 23, 29]. One extends the domain of all multiplicative characters  $\chi$  on  $\mathbb{F}_q^\times$  to  $\mathbb{F}_q$  by defining  $\chi(0) = 0$ . We state a result which enables us to count the number of points on a curve using multiplicative characters on  $\mathbb{F}_p$ .

**Lemma 1.3.6.** [23, Prop. 8.1.5] *Let  $a \in \mathbb{F}_p^\times$ . If  $n|(p - 1)$ , then*

$$\#\{x \in \mathbb{F}_p : x^n = a\} = \sum \chi(a),$$

*where the sum runs over all characters  $\chi$  on  $\mathbb{F}_p$  of order dividing  $n$ .*

We now state the *orthogonality relations* for multiplicative characters in the following lemma. For proofs of these relations and further information on characters, see [23, 6].

**Lemma 1.3.7.** [23, Chap. 8] *Let  $T$  be a fixed generator for the group of multiplicative characters  $\widehat{\mathbb{F}_q^\times}$ . Then*

1.  $\sum_{x \in \mathbb{F}_q} T^n(x) = \begin{cases} q-1 & \text{if } T^n = \varepsilon; \\ 0 & \text{if } T^n \neq \varepsilon. \end{cases}$
2.  $\sum_{n=0}^{q-2} T^n(x) = \begin{cases} q-1 & \text{if } x = 1; \\ 0 & \text{if } x \neq 1. \end{cases}$

**Definition 1.3.1.** For multiplicative characters  $A$  and  $B$  of  $\mathbb{F}_q$ , the Jacobi sum  $J(A, B)$  is defined by

$$J(A, B) := \sum_{x \in \mathbb{F}_q} A(x)B(1-x).$$

Define the additive character  $\theta : \mathbb{F}_q \rightarrow \mathbb{C}^\times$  by  $\theta(\alpha) = \zeta^{\text{tr}(\alpha)}$ . Note that  $\zeta = e^{2\pi i/p}$  and  $\text{tr} : \mathbb{F}_q \rightarrow \mathbb{F}_p$  is the trace map given by

$$\text{tr}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{e-1}}.$$

The following theorem of additive character will be used frequently to express the number of  $\mathbb{F}_q$ -points on polynomials in simplified form.

**Theorem 1.3.8.** [23, Thm. 10.3.3] *Let  $x, y, z \in \mathbb{F}_q$ . Then*

$$\sum_{z \in \mathbb{F}_q} \theta(z(x-y)) = q\delta(x, y), \quad (1.3.1)$$

where  $\delta(x, y) = 1$  if  $x = y$  and zero otherwise.

Further, we define an important character sum called Gauss sum as follows.

**Definition 1.3.2.** For  $A \in \widehat{\mathbb{F}_q^\times}$ , the *Gauss sum* is defined by

$$G(A) := \sum_{x \in \mathbb{F}_q} A(x)\zeta^{\text{tr}(x)} = \sum_{x \in \mathbb{F}_q} A(x)\theta(x).$$

Denoting  $T$  as a fixed generator of  $\widehat{\mathbb{F}_q^\times}$ , we often use the notation  $G_m$  to define  $G(T^m)$ . Now, we restate a lemma which provides us values of certain particular Gauss sums.

**Lemma 1.3.9.** [14, Lemma 2.1] *For  $q = p^e$ ,  $p$  a prime and  $e \in \mathbb{N}$ , we have*

- (a)  $G(\varepsilon) = G_0 = -1$
- (b)  $G(\phi) = G_{\frac{q-1}{2}} = \begin{cases} \sqrt{q}, & \text{if } q \equiv 1 \pmod{4}; \\ i\sqrt{q}, & \text{if } q \equiv 3 \pmod{4}. \end{cases}$

The following lemma enables us to evaluate multiplicative inverse of a Gauss sum.

**Lemma 1.3.10.** [18, Eqn. 1.12] *If  $k \in \mathbb{Z}$  and  $T^k \neq \varepsilon$ , then*

$$G_k G_{-k} = q T^k(-1).$$

Using orthogonality of characters, we have a lemma that provide a scope to express an additive character in terms of Gauss sums.

**Lemma 1.3.11.** [14, Lemma 2.2] *For all  $\alpha \in \mathbb{F}_q^\times$ ,*

$$\theta(\alpha) = \frac{1}{q-1} \sum_{m=0}^{q-2} G_{-m} T^m(\alpha).$$

There are many nice relationships between Gauss sums and Jacobi sums. Among them, the most beautiful one is the following.

**Lemma 1.3.12.** [18, Eqn. 1.14] *If  $T^{m-n} \neq \varepsilon$ , then*

$$G_m G_{-n} = q \binom{T^m}{T^n} G_{m-n} T^n(-1) = J(T^m, T^{-n}) G_{m-n}.$$

### 1.3.3 Gaussian hypergeometric functions

Gaussian hypergeometric series is first introduced by Greene in [18] as finite field analogue of the classical hypergeometric series.

**Definition 1.3.3.** For character  $A$  and  $B$  on  $\mathbb{F}_q$ , the binomial coefficient  $\binom{A}{B}$  is defined by

$$\binom{A}{B} := \frac{B(-1)}{q} J(A, \bar{B}) = \frac{B(-1)}{q} \sum_{x \in \mathbb{F}_q} A(x) \bar{B}(1-x),$$

where  $\bar{B}$  is the inverse of  $B$ .

Many special cases of the binomial coefficient have been deduced by Greene. For example, the following special case is known from [18]

$$\binom{A}{\varepsilon} = \binom{A}{A} = -\frac{1}{q} + \frac{q-1}{q} \delta(A), \quad (1.3.2)$$

where  $\delta(A) = 0$  if  $A \neq \varepsilon$  and  $\delta(A) = 1$  if  $A = \varepsilon$ . With these notation, Greene defined Gaussian hypergeometric series in the following way:

**Definition 1.3.4.** Let  $n$  be any positive integer and  $x \in \mathbb{F}_q$ . For characters  $A_0, A_1, \dots, A_n$  and  $B_1, B_2, \dots, B_n$  in  $\widehat{\mathbb{F}_q^\times}$ , the Gaussian hypergeometric series  ${}_{n+1}F_n$  is defined to be

$${}_{n+1}F_n \left( \begin{matrix} A_0, & A_1, & \dots, & A_n \\ & B_1, & \dots, & B_n \end{matrix} \middle| x \right) := \frac{q}{q-1} \sum_{\chi \in \widehat{\mathbb{F}_q^\times}} \binom{A_0\chi}{\chi} \binom{A_1\chi}{B_1\chi} \dots \binom{A_n\chi}{B_n\chi} \chi(x).$$

Greene also provided an alternative definition of  ${}_2F_1$  Gaussian hypergeometric function as follows.

**Definition 1.3.5.** For character  $A, B, C$  on  $\mathbb{F}_q$  and  $x \in \mathbb{F}_q$ , we have

$${}_2F_1 \left( \begin{matrix} A, & B \\ & C \end{matrix} \middle| x \right) = \varepsilon(x) \frac{BC(-1)}{q} \sum_{y \in \mathbb{F}_q} B(y) \overline{B}C(1-y) \overline{A}(1-xy). \quad (1.3.3)$$

Greene found many symmetric and transformation formulas for Gaussian hypergeometric series analogous to those satisfied by classical hypergeometric series. Some follow directly from his definitions, while others are far more subtle. For characters  $A_1, \dots, A_n$  and  $B_1, \dots, B_n$  on  $\mathbb{F}_q$ , let

$$\begin{pmatrix} \vec{A} \\ \vec{B} \end{pmatrix}$$

denotes the product

$$\prod_{k=1}^n \begin{pmatrix} A_k \\ B_k \end{pmatrix}.$$

Further, let

$$F \left( \begin{matrix} C, & \vec{A} \\ & \vec{B} \end{matrix} \middle| x \right)$$

denotes the series

$${}_{n+1}F_n \left( \begin{matrix} C, & A_1, & \dots, & A_n \\ & B_1, & \dots, & B_n \end{matrix} \middle| x \right).$$

With these notation, we now recall some results of Greene.

**Theorem 1.3.13.** [18, Thm. 3.15 (v)] For characters  $A, B, C, E, \vec{D}, \vec{F}$  on  $\mathbb{F}_q$  and  $x \in \mathbb{F}_q$

$$\begin{aligned} F \left( \begin{matrix} A, & B, & C, & \vec{D} \\ & E, & B, & \vec{F} \end{matrix} \middle| x \right) &= \left( \frac{C\overline{E}}{B\overline{E}} \right) F \left( \begin{matrix} A, & C, & \vec{D} \\ & E, & \vec{F} \end{matrix} \middle| x \right) - \frac{BE(-1)}{q} \overline{B}(x) \begin{pmatrix} A\overline{B} \\ \overline{B} \end{pmatrix} \\ &\quad \times \begin{pmatrix} \vec{D}\overline{B} \\ \vec{F}\overline{B} \end{pmatrix} + \frac{q-1}{q^2} BE(-1) F \left( \begin{matrix} A, & \vec{D} \\ & \vec{B} \end{matrix} \middle| x \right) \delta(C\overline{E}). \end{aligned}$$

**Theorem 1.3.14.** [18, Thm. 4.2 (ii)] For characters  $A, B, D, \vec{C}, \vec{E}$  of  $\mathbb{F}_q$  and  $x \in \mathbb{F}_q$ ,

$$F \left( \begin{matrix} A, & B, & \vec{C} \\ & D, & \vec{E} \end{matrix} \middle| x \right) = ABD\vec{C}\vec{E}(-1)\bar{A}(x)F \left( \begin{matrix} A, & A\bar{D}, & A\vec{E} \\ & A\bar{B}, & A\vec{C} \end{matrix} \middle| \frac{1}{x} \right).$$

Moreover, Greene proved the following transformation formulas of Gaussian hypergeometric series using the binomial theorem of characters and making changes in variables in Definitions 1.3.4 and 1.3.5. Let  $\delta : \mathbb{F}_q \rightarrow \{0, 1\}$  be the function defined by  $\delta(0) = 1$  and  $\delta(x) = 0$  for  $x \neq 0$ .

**Theorem 1.3.15.** [18, Thm. 4.4 (i) & (ii)] For character  $A, B, C$  on  $\mathbb{F}_q$  and  $x \in \mathbb{F}_q$ ,

$$\begin{aligned} (i) \quad {}_2F_1 \left( \begin{matrix} A, & B \\ & C \end{matrix} \middle| x \right) &= A(-1){}_2F_1 \left( \begin{matrix} A, & B \\ & ABC \end{matrix} \middle| 1-x \right) \\ &\quad + A(-1) \binom{B}{AC} \delta(1-x) - \binom{B}{C} \delta(x), \\ (ii) \quad {}_2F_1 \left( \begin{matrix} A, & B \\ & C \end{matrix} \middle| x \right) &= C(-1)\bar{A}(1-x){}_2F_1 \left( \begin{matrix} A, & C\bar{B} \\ & C \end{matrix} \middle| \frac{x}{x-1} \right) \\ &\quad + A(-1) \binom{B}{AC} \delta(1-x). \end{aligned}$$

**Lemma 1.3.16.** [18, Coro. 3.16 (ii)] For characters  $A, B$  on  $\mathbb{F}_q$  and  $x \in \mathbb{F}_q$ ,

$$\begin{aligned} {}_2F_1 \left( \begin{matrix} A, & \varepsilon \\ & B \end{matrix} \middle| x \right) &= \binom{B}{A} A(-1)\bar{B}(x)\bar{A}B(1-x) \\ &\quad - \frac{1}{q} B(-1)\varepsilon(x) + \frac{q-1}{q} A(-1)\delta(1-x)\delta(\bar{A}B). \end{aligned}$$

We will need the Hasse-Davenport relation to express traces of Frobenius endomorphism of elliptic curves as special values of Gaussian hypergeometric series. The Hasse-Davenport relation can be stated as follows. Here  $\theta$  is considered as the additive character though the most general version of this relation involves any additive character.

**Lemma 1.3.17.** [26, Hasse-Davenport Relation] Let  $m$  be a positive integer and let  $q = p^e$  be a prime power such that  $q \equiv 1 \pmod{m}$ . Let  $\theta$  be the additive character on  $\mathbb{F}_q$  defined by  $\theta(\alpha) = \zeta^{\text{tr}(\alpha)}$ , where  $\zeta = e^{\frac{2\pi i}{p}}$ . For multiplicative characters  $\chi, \psi \in \widehat{\mathbb{F}_q^\times}$ , we have

$$\prod_{\chi^m=1} G(\chi\psi) = -G(\psi^m)\psi(m^{-m}) \prod_{\chi^m=1} G(\chi). \quad (1.3.4)$$



## 1.4 Organization

There are six chapters in this thesis. We explore connections that values of hypergeometric functions may have with algebraic curves and polynomials.

The Chapter 1 is introductory in nature which contains basic introduction to algebraic curves, classical hypergeometric series, and Gaussian hypergeometric series. We also give a brief survey of recent works that relates algebraic curves with hypergeometric functions.

Chapter 2 is dedicated to study connections between traces of Frobenius of elliptic curves and Gaussian hypergeometric series. For each of the cases,  $q \equiv 1 \pmod{6}$ ,  $q \equiv 1 \pmod{4}$ , and  $q \equiv 1 \pmod{3}$ , we find explicit relationships between the number of  $\mathbb{F}_q$ -points on certain families of elliptic curves in Weierstrass normal form and the values of a particular hypergeometric function over  $\mathbb{F}_q$ .

In Chapter 3, we focus our attention on a particular family of algebraic curve of higher degree and find connection between the number of points on this family over  $\mathbb{F}_p$  and sums of values of certain  ${}_2F_1$  Gaussian hypergeometric functions. We also provide a striking analogy between binomial coefficients involving rational numbers and those involving multiplicative characters.

Chapter 4 is devoted to another family of algebraic curve of higher degree. We express the number of points on this family of curve over  $\mathbb{F}_q$  as a linear combination of certain  ${}_3F_2$  Gaussian hypergeometric series.

Chapter 5 contains relations between number of zeros on some polynomial equations over  $\mathbb{F}_q$  and  ${}_{n+1}F_n$  Gaussian hypergeometric series for  $n \geq 2$ . These expressions partially answer a question proposed by Ono [35].

Finally, in Chapter 6, we evaluate certain special values of  ${}_2F_1$  and  ${}_3F_2$  Gaussian hypergeometric series over  $\mathbb{F}_q$  using the results of Chapter 2 and Chapter 4.

## Chapter 2

# Elliptic Curves and Gaussian Hypergeometric Series

### 2.1 Introduction

An elliptic curve is a particular family of algebraic curve, which can be described as non-singular cubic projective curve over a field in three variables with at least one point. These curves are of genus 1, and the points on such curves over any field enjoy the beautiful group law of algebra called Mordell-Weil group law [37, 22]. Any elliptic curve over  $\mathbb{Q}$  can be represented by an equation

$$E : y^2 = f(x) = x^3 + ax + b,$$

where  $f(x) = 0$  does not have any repeated roots. This form of an elliptic curve is called the Weierstrass normal form. The discriminant of  $E$ , denoted by  $\Delta(E)$ , is given by

$$\Delta(E) = -16(4a^3 + 27b^2).$$

Let  $\tilde{E}$  denote the reduction of  $E \bmod p$ . Recall that if  $p \nmid \Delta(E)$  then  $E$  has good reduction, that is  $\tilde{E}$  is also an elliptic curve over  $\mathbb{F}_p$ . In this case, we say that  $p$  is a prime of good reduction. We define the integer  $a_p(E)$  by

$$a_p(E) = p + 1 - \#\tilde{E}(\mathbb{F}_p),$$

---

<sup>1</sup>The contents of this chapter have been published in *Proc. Amer. Math. Soc.* (2013) and *J. Number Theory* (2013).

where  $\#\tilde{E}(\mathbb{F}_p)$  is the number of points on  $\tilde{E}$  over  $\mathbb{F}_p$  including the point at infinity. If  $p$  is a prime of good reduction,  $a_p(E)$  is called the trace of Frobenius as it can be interpreted as the trace of the Frobenius endomorphism on  $E$ . Further, if  $E$  is given by  $y^2 = f(x)$  then

$$a_p(E) = - \sum_{x \in \mathbb{F}_p} \phi(f(x)),$$

where  $\phi$  is the quadratic character on  $\mathbb{F}_p$ . For further details about elliptic curves and its different parameters, see [37, 41, 22].

Elliptic curves have many mysterious arithmetic properties and mathematicians are working to find their connections to other objects in number theory and related areas of mathematics. The connection between elliptic curves and modular forms brought to light famously in the proof of Fermat's Last Theorem. There are many open problems on elliptic curves and the most famous is the Birch and Swinnerton-Dyer conjecture.

In this chapter, we consider the problem of expressing traces of Frobenius endomorphisms of certain families of elliptic curves in terms of hypergeometric functions over finite fields. We present explicit relations between the traces of Frobenius endomorphisms of certain families of elliptic curves and special values of  ${}_2F_1$ -hypergeometric functions over  $\mathbb{F}_q$  for  $q \equiv 1 \pmod{6}$ ,  $q \equiv 1 \pmod{4}$ , and  $q \equiv 1 \pmod{3}$ . Moreover, we extend a result of Koike on Legendre's family of elliptic curves which includes some more families of elliptic curves.

## 2.2 Traces of Frobenius endomorphism of elliptic curves

Throughout, we consider an elliptic curve  $E_{a,b,c}$  over  $\mathbb{F}_q$  given by

$$E_{a,b,c} : y^2 = x^3 + ax^2 + bx + c. \tag{2.2.1}$$

If we denote by  $a_q(E_{a,b,c})$  the trace of the Frobenius endomorphism on  $E_{a,b,c}$ , then

$$a_q(E_{a,b,c}) = q + 1 - \#E_{a,b,c}(\mathbb{F}_q), \quad (2.2.2)$$

where  $\#E_{a,b,c}(\mathbb{F}_q)$  represents the number of  $\mathbb{F}_q$ -points on  $E_{a,b,c}$  including the point at infinity. Fuselier [14], Koike [25], Lennon [27, 28], and Ono [34] considered some particular forms of the elliptic curve  $E_{a,b,c}$  and expressed their traces of Frobenius endomorphism in terms of Gaussian hypergeometric series. Among them, Lennon [27] considered the most general form and related its number of points with hypergeometric series over  $\mathbb{F}_q$  containing characters of order 12, as parameters for  $q = p^e \equiv 1 \pmod{12}$ .

In the following theorems, we extend the result for  $a_q(E_{a,b,c})$  of Lennon and deduce some expressions for  $a_q(E_{a,b,c})$  in terms of hypergeometric functions over  $\mathbb{F}_q$  for  $q \equiv 1 \pmod{6}$ ,  $q \equiv 1 \pmod{4}$ , and  $q \equiv 1 \pmod{3}$ , respectively. In the proofs, we follow the method used in [14] and [27].

### 2.2.1 Case 1: $q \equiv 1 \pmod{6}$

**Theorem 2.2.1.** *Let  $q = p^e$ ,  $p > 0$ , be a prime and  $q \equiv 1 \pmod{6}$ . In addition, let  $a$  be non-zero such that  $(-a/3)$  a quadratic residue in  $\mathbb{F}_q$ . If  $T \in \widehat{\mathbb{F}_q^\times}$  is a generator of the character group, then the trace of the Frobenius on  $E_{0,a,b} : y^2 = x^3 + ax + b$  can be expressed as*

$$a_q(E_{0,a,b}) = -qT^{\frac{q-1}{2}}(-k) {}_2F_1 \left( \begin{matrix} T^{\frac{q-1}{6}}, & T^{\frac{5(q-1)}{6}} \\ \varepsilon & \left| -\frac{k^3 + ak + b}{4k^3} \right. \end{matrix} \right),$$

where  $\varepsilon$  is the trivial character on  $\mathbb{F}_q$  and  $k \in \mathbb{F}_q$  satisfies  $3k^2 + a = 0$ .

Theorem 2.2.1 will follow as a consequence of the next theorem. We consider the family of elliptic curves  $E_{c,0,d}$  over  $\mathbb{F}_q$  for  $c \neq 0$ . Then, the trace of the Frobenius endomorphism of  $E_{c,0,d}$  is expressed as a special value of a hypergeometric function in the following way.

**Theorem 2.2.2.** *Let  $q = p^e$ ,  $p > 0$ , be a prime and  $q \equiv 1 \pmod{6}$ . If  $T \in \widehat{\mathbb{F}_q^\times}$  is a generator of the character group, then the trace of the Frobenius on  $E_{c,0,d} : y^2 = x^3 + cx^2 + d$  is given by*

$$a_q(E_{c,0,d}) = -qT^{\frac{q-1}{2}}(-3c) {}_2F_1 \left( \begin{matrix} T^{\frac{q-1}{6}}, & T^{\frac{5(q-1)}{6}} \\ \varepsilon & \end{matrix} \middle| -\frac{27d}{4c^3} \right),$$

where  $\varepsilon$  is the trivial character on  $\mathbb{F}_q$ .

*Proof.* Consider the polynomial

$$P(x, y) = x^3 + cx^2 + d - y^2,$$

and denote by  $\#E_{c,0,d}(\mathbb{F}_q)$  the number of points on the curve  $E_{c,0,d}$  over  $\mathbb{F}_q$  including the point at infinity. Then

$$\#E_{c,0,d}(\mathbb{F}_q) - 1 = \#\{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q : P(x, y) = 0\}.$$

The elementary identity (1.3.1) for the polynomial  $P(x, y)$  becomes

$$\sum_{z \in \mathbb{F}_q} \theta(zP(x, y)) = \begin{cases} q & \text{if } P(x, y) = 0; \\ 0 & \text{if } P(x, y) \neq 0. \end{cases} \quad (2.2.3)$$

Using this, we obtain

$$\begin{aligned} q \cdot (\#E_{c,0,d}(\mathbb{F}_q) - 1) &= \sum_{x, y, z \in \mathbb{F}_q} \theta(zP(x, y)) \\ &= \sum_{x, y \in \mathbb{F}_q} \theta(0P(x, y)) + \sum_{z \in \mathbb{F}_q^\times} \theta(zP(0, 0)) + \sum_{y, z \in \mathbb{F}_q^\times} \theta(zP(0, y)) \\ &\quad + \sum_{x, z \in \mathbb{F}_q^\times} \theta(zP(x, 0)) + \sum_{x, y, z \in \mathbb{F}_q^\times} \theta(zP(x, y)). \end{aligned}$$

The polynomial  $P(x, y)$  and the fact

$$\sum_{x, y \in \mathbb{F}_q} \theta(0P(x, y)) = \sum_{x, y \in \mathbb{F}_q} \theta(0) = q^2,$$

together yield

$$\begin{aligned}
q \cdot (\#E_{c,0,d}(\mathbb{F}_q) - 1) &= q^2 + \sum_{z \in \mathbb{F}_q^\times} \theta(zd) + \sum_{y, z \in \mathbb{F}_q^\times} \theta(zd)\theta(-zy^2) + \\
&\quad \sum_{x, z \in \mathbb{F}_q^\times} \theta(zd)\theta(zx^3)\theta(zcx^2) + \sum_{x, y, z \in \mathbb{F}_q^\times} \theta(zd)\theta(zx^3)\theta(zcx^2)\theta(-zy^2) \\
&:= q^2 + A + B + C + D. \tag{2.2.4}
\end{aligned}$$

Now using Lemma 1.3.11 and then applying Lemma 1.3.7 repeatedly for each labeled term of (2.2.4), we deduce that

$$A = \frac{1}{q-1} \sum_{z \in \mathbb{F}_q^\times} \sum_{l=0}^{q-2} G_{-l} T^l(zd) = \frac{1}{q-1} \sum_{l=0}^{q-2} G_{-l} T^l(d) \sum_{z \in \mathbb{F}_q^\times} T^l(z) = G_0 = -1.$$

Here the second equality follows from the fact that the innermost sum is 0 unless  $l = 0$ , at which it is  $q - 1$ . Similarly,

$$B = \frac{1}{(q-1)^2} \sum_{l, m=0}^{q-2} G_{-l} G_{-m} T^l(d) T^m(-1) \sum_{y \in \mathbb{F}_q^\times} T^{2m}(y) \sum_{z \in \mathbb{F}_q^\times} T^{l+m}(z),$$

which is nonzero if and only if  $l = -m$  and  $m = 0$  or  $\frac{q-1}{2}$ . Thus, Lemma 1.3.7 yields

$$B = 1 + G_{\frac{q-1}{2}} G_{-\frac{q-1}{2}} T^{\frac{q-1}{2}}(d) T^{\frac{q-1}{2}}(-1).$$

Using Lemma 1.3.10 for  $k = \frac{q-1}{2}$ , we deduce that

$$\begin{aligned}
B &= 1 + q T^{\frac{q-1}{2}}(-1) T^{\frac{q-1}{2}}(d) T^{\frac{q-1}{2}}(-1) \\
&= 1 + q T^{\frac{q-1}{2}}(d).
\end{aligned}$$

Expanding the next term, we have

$$C = \frac{1}{(q-1)^3} \sum_{l, m, n=0}^{q-2} G_{-l} G_{-m} G_{-n} T^l(d) T^m(c) \sum_{z \in \mathbb{F}_q^\times} T^{l+m+n}(z) \sum_{x \in \mathbb{F}_q^\times} T^{3m+2n}(x).$$

Finally,

$$\begin{aligned}
D &= \frac{1}{(q-1)^4} \sum_{l, m, n, k=0}^{q-2} G_{-l} G_{-m} G_{-n} G_{-k} T^l(d) T^m(c) T^k(-1) \times \\
&\quad \sum_{z \in \mathbb{F}_q^\times} T^{l+m+n+k}(z) \sum_{x \in \mathbb{F}_q^\times} T^{3m+2n}(x) \sum_{z \in \mathbb{F}_q^\times} T^{2k}(z).
\end{aligned}$$

The innermost sum of  $D$  is nonzero only when  $k = 0$  or  $k = \frac{q-1}{2}$ . Using the fact that  $G_0 = -1$ , we obtain

$$D = -C + D_{\frac{q-1}{2}},$$

where

$$D_{\frac{q-1}{2}} = \frac{1}{(q-1)^3} \sum_{l,m,n=0}^{q-2} G_{-l}G_{-m}G_{-n}G_{\frac{q-1}{2}} T^l(d)T^m(c)T^{\frac{q-1}{2}}(-1) \times \\ \sum_{z \in \mathbb{F}_q^\times} T^{l+m+n+\frac{q-1}{2}}(z) \sum_{x \in \mathbb{F}_q^\times} T^{3m+2n}(x),$$

which is zero unless  $m = -\frac{2}{3}n$  and  $n = -3l - \frac{3(q-1)}{2}$ . Since  $G_{3l+\frac{3(q-1)}{2}} = G_{3l+\frac{q-1}{2}}$  and  $G_{-2l-(q-1)} = G_{-2l}$ , we have

$$D_{\frac{q-1}{2}} = \frac{1}{q-1} \sum_{l=0}^{q-2} G_{-l}G_{-2l}G_{3l+\frac{q-1}{2}}G_{\frac{q-1}{2}} T^l(d)T^{-3l+\frac{q-1}{2}}(c)T^{\frac{q-1}{2}}(-1).$$

Using Davenport-Hasse relation (1.3.4) for  $m = 2, \psi = T^{-l}$  and  $m = 3, \psi = T^{l+\frac{q-1}{6}}$  respectively, we deduce that

$$G_{-2l} = \frac{G_{-l}G_{-l-\frac{q-1}{2}}}{G_{\frac{q-1}{2}}T^l(4)} \quad \text{and} \quad G_{3l+\frac{q-1}{2}} = \frac{G_{l+\frac{q-1}{6}}G_{l+\frac{q-1}{2}}G_{l+\frac{5(q-1)}{6}}}{qT^{-l-\frac{q-1}{6}}(27)}.$$

Therefore,

$$D_{\frac{q-1}{2}} = \frac{T^{\frac{q-1}{2}}(-3c)}{q(q-1)} \sum_{l=0}^{q-2} G_{-l}G_{-l}G_{-l-\frac{q-1}{2}}G_{l+\frac{q-1}{6}}G_{l+\frac{q-1}{2}}G_{l+\frac{5(q-1)}{6}} T^l \left( \frac{27d}{4c^3} \right).$$

Replacing  $l$  by  $l - \frac{q-1}{2}$ , we have

$$D_{\frac{q-1}{2}} = \frac{T^{\frac{q-1}{2}}(-3c)}{q(q-1)} \sum_{l=0}^{q-2} G_{-l+\frac{q-1}{2}}G_{-l+\frac{q-1}{2}}G_{-l}G_{l-\frac{q-1}{3}}G_lG_{l+\frac{q-1}{3}} T^{l-\frac{q-1}{2}} \left( \frac{27d}{4c^3} \right).$$

Now using Lemma 1.3.12, we obtain

$$D_{\frac{q-1}{2}} = \frac{qT^{\frac{q-1}{2}}(-3c)}{q-1} \sum_{l=0}^{q-2} G_lG_{-l} \left( \frac{T^{l-\frac{q-1}{3}}}{T^{l-\frac{q-1}{2}}} \right) G_{\frac{q-1}{6}} \left( \frac{T^{l+\frac{q-1}{3}}}{T^{l-\frac{q-1}{2}}} \right) G_{\frac{5(q-1)}{6}} T^{l-\frac{q-1}{2}} \left( \frac{27d}{4c^3} \right).$$

Plugging the facts that if  $l \neq 0$  then  $G_l G_{-l} = qT^l(-1)$  and if  $l = 0$  then  $G_l G_{-l} = qT^l(-1) - (q-1)$  in appropriate identities for each  $l$ , we deduce that

$$D_{\frac{q-1}{2}} = \frac{q^3 T^{\frac{q-1}{6}}(-1) T^{\frac{q-1}{2}}(-3c)}{q-1} \sum_{l=0}^{q-2} \begin{pmatrix} T^{l-\frac{q-1}{3}} \\ T^{l-\frac{q-1}{2}} \end{pmatrix} \begin{pmatrix} T^{l+\frac{q-1}{3}} \\ T^{l-\frac{q-1}{2}} \end{pmatrix} T^{l-\frac{q-1}{2}} \left( \frac{27d}{4c^3} \right) T^l(-1) \\ - q^2 T^{\frac{q-1}{6}}(-1) T^{\frac{q-1}{2}}(-3c) \begin{pmatrix} T^{\frac{2(q-1)}{3}} \\ T^{\frac{q-1}{2}} \end{pmatrix} \begin{pmatrix} T^{\frac{q-1}{3}} \\ T^{\frac{q-1}{2}} \end{pmatrix} T^{\frac{q-1}{2}} \left( \frac{27d}{4c^3} \right).$$

Replacing  $l$  by  $l + \frac{q-1}{2}$  in the first term and simplifying the second term, we obtain

$$D_{\frac{q-1}{2}} = \frac{q^3 T^{\frac{q-1}{2}}(-3c)}{q-1} \sum_{l=0}^{q-2} \begin{pmatrix} T^{l+\frac{q-1}{6}} \\ T^l \end{pmatrix} \begin{pmatrix} T^{l+\frac{5(q-1)}{6}} \\ T^l \end{pmatrix} T^l \left( -\frac{27d}{4c^3} \right) \\ - q^2 T^{\frac{q-1}{2}}(d) \frac{G_{\frac{2(q-1)}{3}} G_{\frac{q-1}{2}} G_{\frac{q-1}{3}} G_{\frac{q-1}{2}}}{q^2 G_{\frac{q-1}{6}} G_{\frac{5(q-1)}{6}}} \\ = q^2 T^{\frac{q-1}{2}}(-3c) {}_2F_1 \left( \begin{matrix} T^{\frac{q-1}{6}}, & T^{\frac{5(q-1)}{6}} \\ & \varepsilon \end{matrix} \middle| -\frac{27d}{4c^3} \right) - q T^{\frac{q-1}{2}}(d).$$

Putting the values of  $A, B, C, D$  all together in (2.2.4), we have

$$q \cdot (\#E_{c,0,d}(\mathbb{F}_q) - 1) = q^2 + q^2 T^{\frac{q-1}{2}}(-3c) {}_2F_1 \left( \begin{matrix} T^{\frac{q-1}{6}}, & T^{\frac{5(q-1)}{6}} \\ & \varepsilon \end{matrix} \middle| -\frac{27d}{4c^3} \right).$$

Since  $a_q(E_{c,0,d}) = q + 1 - \#E_{c,0,d}(\mathbb{F}_q)$ , we have completed the proof of the Theorem.  $\square$

**Proof of Theorem 2.2.1.** Since  $a \neq 0$  and  $(-a/3)$  is quadratic residue in  $\mathbb{F}_q$ , we find  $k \in \mathbb{F}_q^\times$  such that  $3k^2 + a = 0$ . A change of variables  $(x, y) \mapsto (x+k, y)$  takes the elliptic curve  $E_{0,a,b} : y^2 = x^3 + ax + b$  to

$$E_{a',0,b'} : y^2 = x^3 + 3kx^2 + (k^3 + ak + b),$$

where  $a' = 3k^2$  and  $b' = k^3 + ak + b$ . Clearly  $a_q(E_{0,a,b}) = a_q(E_{a',0,b'})$ . Since  $3k \neq 0$ , using Theorem 2.2.2 for the elliptic curve  $E_{a',0,b'}$ , we complete the proof.  $\square$



### 2.2.2 Case 2: $q \equiv 1 \pmod{4}$

**Theorem 2.2.3.** *Let  $q = p^e$ ,  $p > 3$ , be a prime and  $q \equiv 1 \pmod{4}$ . Also assume that  $x^3 + ax + b = 0$  has a non-zero solution in  $\mathbb{F}_q$  and  $T \in \widehat{\mathbb{F}_q^\times}$  is a generator of the character group. The trace of the Frobenius on  $E_{0,a,b} : y^2 = x^3 + ax + b$  can be expressed as*

$$a_q(E_{0,a,b}) = -qT^{\frac{q-1}{2}}(6h)T^{\frac{q-1}{4}}(-1) {}_2F_1 \left( \begin{matrix} T^{\frac{q-1}{4}}, & T^{\frac{3(q-1)}{4}} \\ \varepsilon & \left| \frac{12h^2 + 4a}{9h^2} \right. \end{matrix} \right),$$

where  $\varepsilon$  is the trivial character of  $\mathbb{F}_q$  and  $h \in \mathbb{F}_q^\times$  satisfies  $h^3 + ah + b = 0$ .

We now prove a result for the elliptic curve  $E_{f,g,0} : y^2 = x^3 + fx^2 + gx$  under the condition that  $q \equiv 1 \pmod{4}$  similar to Theorem 2.2.2, and then Theorem 2.2.3 will follow from this result.

**Theorem 2.2.4.** *Let  $q = p^e$ ,  $p > 0$ , be a prime and  $q \equiv 1 \pmod{4}$ . If  $T \in \widehat{\mathbb{F}_q^\times}$  is a generator of the character group and  $f \neq 0$ , then the trace of the Frobenius on  $E_{f,g,0}$  is given by*

$$a_q(E_{f,g,0}) = -qT^{\frac{q-1}{2}}(2f)T^{\frac{q-1}{4}}(-1) {}_2F_1 \left( \begin{matrix} T^{\frac{q-1}{4}}, & T^{\frac{3(q-1)}{4}} \\ \varepsilon & \left| \frac{4g}{f^2} \right. \end{matrix} \right),$$

where  $\varepsilon$  is the trivial character on  $\mathbb{F}_q$ .

*Proof.* We have

$$\#E_{f,g,0}(\mathbb{F}_q) - 1 = \#\{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q : P(x, y) = 0\},$$

where

$$P(x, y) = x^3 + fx^2 + gx - y^2.$$

Using (2.2.3), we express the number of points of  $E_{f,g,0}$  over  $\mathbb{F}_q$  as

$$\begin{aligned}
q \cdot (\#E_{f,g,0}(\mathbb{F}_q) - 1) &= \sum_{x,y,z \in \mathbb{F}_q} \theta(zP(x,y)) \\
&= q^2 + \sum_{z \in \mathbb{F}_q^\times} \theta(0) + \sum_{y,z \in \mathbb{F}_q^\times} \theta(-zy^2) + \sum_{x,z \in \mathbb{F}_q^\times} \theta(zx^3)\theta(zfx^2)\theta(zgx) \\
&\quad + \sum_{x,y,z \in \mathbb{F}_q^\times} \theta(zx^3)\theta(zfx^2)\theta(zgx)\theta(-zy^2) \\
&:= q^2 + (q-1) + A + B + C.
\end{aligned} \tag{2.2.5}$$

Now, following the same procedure as followed in the proof of Theorem 2.2.2, we deduce that

$$A = \frac{1}{q-1} \sum_{l=0}^{q-2} \sum_{y,z \in \mathbb{F}_q^\times} G_l T^l(-zy^2) = \frac{1}{q-1} \sum_{l=0}^{q-2} G_l \sum_{y \in \mathbb{F}_q} T^{2l}(y) \sum_{z \in \mathbb{F}_q} T^l(-z) = -(q-1),$$

where the third equality follows from the fact that the innermost sums are nonzero only for  $l = 0$ , at which both are  $q-1$  and  $G_0 = -1$ . Then expanding the next term, we obtain

$$B = \frac{1}{(q-1)^3} \sum_{l,m,n=0}^{q-2} G_{-l} G_{-m} G_{-n} T^m(f) T^n(g) \sum_{z \in \mathbb{F}_q^\times} T^{l+m+n}(z) \sum_{x \in \mathbb{F}_q^\times} T^{3l+2m+n}(x)$$

Finally, using Lemma 1.3.11 and Lemma 1.3.7 in the last term of (2.2.5), we deduce that

$$\begin{aligned}
C &= \frac{1}{(q-1)^4} \sum_{l,m,n=0}^{q-2} G_{-l} G_{-m} G_{-n} G_{-k} T^m(f) T^n(g) T^k(-1) \sum_{z \in \mathbb{F}_q^\times} T^{l+m+n+k}(z) \times \\
&\quad \sum_{x \in \mathbb{F}_q^\times} T^{3l+2m+n}(x) \sum_{y \in \mathbb{F}_q} T^{2k}(y),
\end{aligned}$$

which is nonzero only if  $k = 0$  or  $\frac{q-1}{2}$ . Hence the term breaks up into two terms as

$$\begin{aligned} C = & -\frac{1}{(q-1)^3} \sum_{l,m,n=0}^{q-2} G_{-l}G_{-m}G_{-n}T^m(f)T^n(g) \sum_{z \in \mathbb{F}_q^\times} T^{l+m+n}(z) \sum_{x \in \mathbb{F}_q^\times} T^{3l+2m+n}(x) \\ & + \frac{1}{(q-1)^3} \sum_{l,m,n=0}^{q-2} G_{-l}G_{-m}G_{-n}G_{\frac{q-1}{2}}T^m(f)T^n(g) \sum_{z \in \mathbb{F}_q^\times} T^{l+m+n+\frac{q-1}{2}}(z) \times \\ & \sum_{x \in \mathbb{F}_q^\times} T^{3l+2m+n}(x). \end{aligned}$$

Substituting the values of  $A$ ,  $B$ ,  $C$  all together in (2.2.5), we have

$$\begin{aligned} q \cdot (\#E_{f,g,0}(\mathbb{F}_q) - 1) = & q^2 + \frac{1}{(q-1)^3} \sum_{l,m,n=0}^{q-2} G_{-l}G_{-m}G_{-n}G_{\frac{q-1}{2}}T^m(f)T^n(g) \times \\ & \sum_{z \in \mathbb{F}_q^\times} T^{l+m+n+\frac{q-1}{2}}(z) \sum_{x \in \mathbb{F}_q^\times} T^{3l+2m+n}(x). \end{aligned}$$

Both inner sums of the second term is nonzero only when  $n = l$  and  $m = -2l - \frac{q-1}{2}$ .

Thus, we use Lemma 1.3.7 in the second term, and then simplify to obtain

$$q \cdot (\#E_{f,g,0}(\mathbb{F}_q) - 1) = q^2 + \frac{G_{\frac{q-1}{2}}T^{\frac{q-1}{2}}(f)}{q-1} \sum_{l=0}^{q-2} G_{-l}G_{2l+\frac{q-1}{2}}G_{-l}T^l \left( \frac{g}{f^2} \right). \quad (2.2.6)$$

The Davenport-Hasse relation (1.3.4) with  $m = 2$ ,  $\psi = T^{l+\frac{q-1}{4}}$  yields

$$G_{2l+\frac{q-1}{2}} = \frac{G_{l+\frac{q-1}{4}}G_{l+\frac{3(q-1)}{4}}}{G_{\frac{q-1}{2}}} T^{l-\frac{q-1}{4}}(4). \quad (2.2.7)$$

Using (2.2.7) and then Lemma 1.3.12 in (2.2.6), we have

$$\begin{aligned} q \cdot (\#E_{f,g,0}(\mathbb{F}_q) - 1) & = q^2 + \frac{T^{\frac{q-1}{2}}(2f)}{q-1} \sum_{l=0}^{q-2} G_{-l}G_{l+\frac{q-1}{4}}G_{l+\frac{3(q-1)}{4}}G_{-l}T^l \left( \frac{4g}{f^2} \right) \\ & = q^2 + \frac{q^3 T^{\frac{q-1}{2}}(2f) T^{\frac{q-1}{4}}(-1)}{q-1} \sum_{l=0}^{q-2} \begin{pmatrix} T^{l+\frac{q-1}{4}} \\ T^l \end{pmatrix} \begin{pmatrix} T^{l+\frac{3(q-1)}{4}} \\ T^l \end{pmatrix} T^l \left( \frac{4g}{f^2} \right) \\ & = q^2 + q^2 T^{\frac{q-1}{2}}(2f) T^{\frac{q-1}{4}}(-1) {}_2F_1 \left( \begin{matrix} T^{\frac{q-1}{4}}, T^{\frac{3(q-1)}{4}} \\ \varepsilon \end{matrix} \middle| \frac{4g}{f^2} \right). \end{aligned}$$

Then using the relation  $a_q(E_{f,g,0}) = q + 1 - \#E_{f,g,0}(\mathbb{F}_q)$ , we complete the proof.  $\square$

**Proof of Theorem 2.2.3.** Since  $x^3 + ax + b = 0$  has a non-zero solution in  $\mathbb{F}_q$ , let  $h \in \mathbb{F}_q^\times$  be such that  $h^3 + ah + b = 0$ . A change of variables  $(x, y) \mapsto (x + h, y)$  takes the elliptic curve  $E_{0,a,b} : y^2 = x^3 + ax + b$  to

$$E_{a',b',0} : y^2 = x^3 + 3hx^2 + (3h^2 + a)x,$$

where  $a' = 3h$  and  $b' = 3h^2 + a$ . Since  $a_q(E_{0,a,b}) = a_q(E_{a',b',0})$  and  $3h \neq 0$ , using Theorem 2.2.4 for the elliptic curve  $E_{a',b',0}$ , we complete the proof of the theorem.  $\square$

### 2.2.3 Case 3: $q \equiv 1 \pmod{3}$

In Theorem 2.2.1 and Theorem 2.2.3, we expressed the trace of Frobenius of the elliptic curve  $E_{0,a,b}$  in terms of Gaussian hypergeometric series involving characters of orders 6 and 4 under certain conditions. But all these expressions are not adequate to find trace of Frobenius formula for all families of elliptic curves in terms of Gaussian hypergeometric series because of the conditions imposed on the coefficients of the model. Here we consider a family of elliptic curves which is not included in above theorems and find relation of its number of points with hypergeometric function over finite fields.

**Hessian form of elliptic curve:** Hessian form of elliptic curve is a particular family of elliptic curves. For some  $a \in \mathbb{F}_q$  and  $a^3 \neq 1$ , the Hessian curve over  $\mathbb{F}_q$  is given by the cubic equation

$$C_a : x^3 + y^3 + 1 = 3axy.$$

A birrational change of variables, the equation  $C_a$  transforms to a Weierstrass normal form of elliptic curves.

In the following theorem, we express the number of points on  $C_a$  over  $\mathbb{F}_q$  in terms of Gaussian hypergeometric series. Let  $C_a(\mathbb{F}_q)$  denotes the set of all  $\mathbb{F}_q$ -points on  $C_a$  given by

$$C_a(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q^2 : x^3 + y^3 + 1 = 3axy\}.$$

**Theorem 2.2.5.** *Let  $q = p^e$ ,  $p > 0$ , be a prime and  $q \equiv 1 \pmod{3}$ . If  $T \in \widehat{\mathbb{F}_q^\times}$  is a generator of the character group, then the number of  $\mathbb{F}_q$ -points on the Hessian form of elliptic curve can be expressed as*

$$\#C_a(\mathbb{F}_q) = q - 2 + q \, {}_2F_1 \left( \begin{matrix} T^{\frac{q-1}{3}}, & T^{\frac{2(q-1)}{3}} \\ & \varepsilon \end{matrix} \middle| \frac{1}{a^3} \right).$$

*Proof.* The method of this proof follows similarly to that given in [14] and [27]. We have

$$\#C_a(\mathbb{F}_q) = \#\{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q : P(x, y) = 0\},$$

where

$$P(x, y) = x^3 + y^3 + 1 - 3axy.$$

Using (2.2.3), we express the number of points as

$$\begin{aligned} q \cdot \#C_a(\mathbb{F}_q) &= \sum_{x, y, z \in \mathbb{F}_q} \theta(zP(x, y)) \\ &= q^2 + \sum_{z \in \mathbb{F}_q^\times} \theta(z) + \sum_{y, z \in \mathbb{F}_q^\times} \theta(zy^3)\theta(z) + \sum_{x, z \in \mathbb{F}_q^\times} \theta(zx^3)\theta(z) \\ &\quad + \sum_{x, y, z \in \mathbb{F}_q^\times} \theta(zx^3)\theta(zy^3)\theta(z)\theta(-3azxy) \\ &:= q^2 + (-1) + A + B + C. \end{aligned} \tag{2.2.8}$$

Following the same procedure as followed in the proof of Theorem 2.2.2 and Theorem 2.2.4, we deduce that

$$A = \frac{1}{(q-1)^2} \sum_{l, m=0}^{q-2} \sum_{y, z \in \mathbb{F}_q^\times} G_{-l} G_{-m} T^{l+m}(z) T^{3l}(y) = \frac{1}{q-1} \sum_{l=0}^{q-2} G_{-l} G_l \sum_{y \in \mathbb{F}_q^\times} T^{3l}(y).$$

By Lemma 1.3.7, the above sum is nonzero only if  $l = 0, \frac{q-1}{3}$  or  $\frac{2(q-1)}{3}$ . Thus, using Lemma 1.3.9 (a) and Lemma 1.3.10, we obtain

$$A = G_0 G_0 + G_{\frac{q-1}{3}} G_{\frac{2(q-1)}{3}} + G_{\frac{2(q-1)}{3}} G_{\frac{q-1}{3}} = 1 + 2q.$$

Similarly,

$$B = 1 + 2q.$$

Again, we use Lemma 1.3.11 and Lemma 1.3.7 repeatedly to deduce

$$\begin{aligned} C &= \frac{1}{(q-1)^4} \sum_{l,m,n,k=0}^{q-2} G_{-l}G_{-m}G_{-n}G_{-k}T^k(-3a) \times \\ &\quad \sum_{z \in \mathbb{F}_q^\times} T^{l+m+n+k}(z) \sum_{x \in \mathbb{F}_q^\times} T^{3m+k}(x) \sum_{y \in \mathbb{F}_q^\times} T^{3n+k}(y) \\ &= \frac{1}{(q-1)} \sum_{l=0}^{q-2} G_{-l}G_{-l}G_{-l}G_{3l}T^{-3l}(-3a) + \\ &\quad \frac{2}{(q-1)} \sum_{l=0}^{q-2} G_{-l}G_{-l-\frac{q-1}{3}}G_{-l-\frac{2(q-1)}{3}}G_{3l}T^{-3l}(-3a), \end{aligned}$$

since the sums are nonzero only for  $m = 0, \frac{q-1}{3}$  or  $\frac{2(q-1)}{3}$ ,  $n = 2m - l$  and  $k = -l - m - n$ . We use the Davenport-Hasse relation (1.3.4) for  $G_{3l}$  given as

$$G_{3l} = \frac{G_l G_{l+\frac{q-1}{3}} G_{l+\frac{2(q-1)}{3}}}{qT^{-l}(27)T^{\frac{q-1}{3}}(-1)}$$

in each term, and then Lemma 1.3.12 in the first term to obtain

$$\begin{aligned} C &= \frac{1}{q(q-1)} \sum_{l=0}^{q-2} G_l G_{-l} \left\{ G_{-l} G_{l+\frac{q-1}{3}} \right\} \left\{ G_{-l} G_{l+\frac{2(q-1)}{3}} \right\} T^l \left( -\frac{1}{a^3} \right) \\ &\quad + \frac{2}{q(q-1)} \sum_{l=0}^{q-2} \left\{ G_l G_{-l} \right\} \left\{ G_{l+\frac{q-1}{3}} G_{-(l+\frac{q-1}{3})} \right\} \left\{ G_{l+\frac{2(q-1)}{3}} G_{-(l+\frac{2(q-1)}{3})} \right\} T^l \left( -\frac{1}{a^3} \right) \\ &= \frac{q}{(q-1)} \sum_{l=0}^{q-2} G_l G_{-l} \begin{pmatrix} T^{l+\frac{q-1}{3}} \\ T^l \end{pmatrix} \begin{pmatrix} T^{l+\frac{2(q-1)}{3}} \\ T^l \end{pmatrix} G_{\frac{q-1}{3}} G_{\frac{2(q-1)}{3}} T^l \left( -\frac{1}{a^3} \right) + \frac{2}{q(q-1)} \times \\ &\quad \sum_{l=1, l \neq \frac{q-1}{3}, \frac{2(q-1)}{3}}^{q-2} \left\{ G_l G_{-l} \right\} \left\{ G_{l+\frac{q-1}{3}} G_{-(l+\frac{q-1}{3})} \right\} \left\{ G_{l+\frac{2(q-1)}{3}} G_{-(l+\frac{2(q-1)}{3})} \right\} T^l \left( -\frac{1}{a^3} \right) \\ &\quad + \frac{6}{q(q-1)} G_{\frac{q-1}{3}} G_{-\frac{q-1}{3}} G_{\frac{2(q-1)}{3}} G_{-\frac{2(q-1)}{3}}. \end{aligned}$$

We use Lemma 1.3.10 in each term, and plug the facts that if  $l \neq 0$  then  $G_l G_{-l} = qT^l(-1)$  and if  $l = 0$  then  $G_l G_{-l} = qT^l(-1) - (q-1)$  in appropriate identities for

each  $l$  in the first sum to deduce that

$$\begin{aligned}
C &= \frac{q^3}{(q-1)} \sum_{l=0}^{q-2} \begin{pmatrix} T^{l+\frac{q-1}{3}} \\ T^l \end{pmatrix} \begin{pmatrix} T^{l+\frac{2(q-1)}{3}} \\ T^l \end{pmatrix} T^l \left( \frac{1}{a^3} \right) - q^2 \begin{pmatrix} T^{\frac{q-1}{3}} \\ \varepsilon \end{pmatrix} \begin{pmatrix} T^{\frac{2(q-1)}{3}} \\ \varepsilon \end{pmatrix} \\
&\quad + \frac{2q^2}{(q-1)} \sum_{l=1, l \neq \frac{q-1}{3}, \frac{2(q-1)}{3}}^{q-2} T^l \left( \frac{1}{a^3} \right) + \frac{6q}{q-1}. \\
&= q^2 {}_2F_1 \left( \begin{matrix} T^{\frac{q-1}{3}}, & T^{\frac{2(q-1)}{3}} \\ & \varepsilon \end{matrix} \middle| \frac{1}{a^3} \right) - 1 + \frac{2q^2}{(q-1)} \left[ \left\{ \sum_{l=0}^{q-2} T^l \left( \frac{1}{a^3} \right) \right\} - 3 \right] + \frac{6q}{q-1} \\
&= q^2 {}_2F_1 \left( \begin{matrix} T^{\frac{q-1}{3}}, & T^{\frac{2(q-1)}{3}} \\ & \varepsilon \end{matrix} \middle| \frac{1}{a^3} \right) - 1 - 6q.
\end{aligned}$$

Combining all the values of  $A, B, C$  and putting in (2.2.8), we obtain that

$$q \cdot \#C_a(\mathbb{F}_q) = q^2 - 2q + q^2 {}_2F_1 \left( \begin{matrix} T^{\frac{q-1}{3}}, & T^{\frac{2(q-1)}{3}} \\ & \varepsilon \end{matrix} \middle| \frac{1}{a^3} \right),$$

completing the proof of the theorem.  $\square$

The Hessian form of an elliptic curve can be transform to an elliptic curve in Weierstrass form by making a birational change of variables. Therefore we have the following result.

**Theorem 2.2.6.** *Let  $q = p^e$ ,  $p > 3$ , be a prime with  $q \equiv 1 \pmod{3}$ . In addition, let  $m = -27d(d^3 + 8)$  and  $n = 27(d^6 - 20d^3 - 8)$ , where  $d^3 \neq 1$ . If  $T \in \widehat{\mathbb{F}_q^\times}$  is a generator of the character group, then the trace of the Frobenius on  $E_{0,m,n} : y^2 = x^3 + mx + n$  is given by*

$$a_q(E_{0,m,n}) = 1 + q - \phi(-3(8 + 92d^3 + 35d^6)) - q {}_2F_1 \left( \begin{matrix} T^{\frac{q-1}{3}}, & T^{\frac{2(q-1)}{3}} \\ & \varepsilon \end{matrix} \middle| \frac{1}{d^3} \right).$$

*Proof.* Consider the elliptic curve

$$E_{0,m,n} : y^2 = x^3 + mx + n,$$

where  $m = -27d(d^3 + 8)$  and  $n = 27(d^6 - 20d^3 - 8)$ . Making the birational change of variables  $x \rightarrow -\frac{36-9d^3+3dx-y}{6(9d^2+x)}$  and  $y \rightarrow -\frac{36-9d^3+3dx+y}{6(9d^2+x)}$ , we obtain the equivalent form  $C_d$  (see [13]). Now, the points on  $E_{0,m,n}$  for  $x = -9d^2$  do not correspond to any point on  $C_d$ . Thus there are  $1 + \phi(-3(8 + 92d^3 + 35d^6))$  extra points on  $E_{0,m,n}$ .

On the other hand, under the inverse transformation

$$x \rightarrow \frac{12(d^3 - 1)}{d + x + y} - 9d^2, \quad y \rightarrow \frac{36(d^3 - 1)}{d + x + y}(y - x),$$

the Hesssian curve  $C_d$  is birationally equivalent to  $E_{0,m,n}$ . In this case, the points on  $C_d$  for  $x + y + d = 0$  do not correspond to any point on  $E_{0,m,n}$  and there are  $q$  such extra points. Therefore, we have

$$\#E_{0,m,n}(\mathbb{F}_q) + q = \#C_d(\mathbb{F}_q) + 2 + \phi(-3(8 + 92d^3 + 35d^6)),$$

and hence Theorem 2.2.5 yields

$$\#E_{0,m,n}(\mathbb{F}_q) = \phi(-3(8 + 92d^3 + 35d^6)) + q {}_2F_1 \left( \begin{matrix} T^{\frac{q-1}{3}}, & T^{\frac{2(q-1)}{3}} \\ \epsilon & \mid \frac{1}{d^3} \end{matrix} \right).$$

Finally, using the fact that  $a_q(E_{0,m,n}) = 1 + q - \#E_{0,m,n}(\mathbb{F}_q)$ , we complete the proof.  $\square$

## 2.3 Number of $\mathbb{F}_q$ -points on Edward form of elliptic curve

We are now going to express the number of  $\mathbb{F}_q$ -points on Edward form of elliptic curve in terms of Gaussian hypergeometric series. Later this expression will be used to determine certain special values of Gaussian hypergeometric series.

**Edward form of elliptic curves:** An Edward curve over a finite field  $\mathbb{F}_q$  with characteristic not equal to 2 is given by

$$x^2 + y^2 = u^2(1 + x^2y^2),$$



where  $u \in \mathbb{F}_q$  with  $u^5 \neq u$ . The twisted Edward curve is given by the equation

$$C_{a,b} : ax^2 + y^2 = 1 + bx^2y^2,$$

where  $a$  and  $b$  are distinct nonzero elements of  $\mathbb{F}_q$  (see [7]). This curve has great interest in cryptography. We express the number of  $\mathbb{F}_q$ -points on  $C_{a,b}$  in terms of Gaussian hypergeometric series. Let

$$C_{a,b}(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q^2 : ax^2 + y^2 = 1 + bx^2y^2\}$$

be the set of all  $\mathbb{F}_q$ -points on  $C_{a,b}$ .

**Theorem 2.3.1.** *Let  $q = p^e$ ,  $p > 0$ , be an odd prime and let  $T$  be a generator of the character group  $\widehat{\mathbb{F}_q^\times}$ . The number of points on the twisted Edward curve  $C_{a,b}$  over  $\mathbb{F}_q$  can be expressed as*

$$\#C_{a,b}(\mathbb{F}_q) = \zeta(a, b) + qT^{\frac{q-1}{2}}(-a) {}_2F_1 \left( \begin{matrix} T^{\frac{q-1}{2}}, & T^{\frac{q-1}{2}} \\ & \varepsilon \end{matrix} \middle| \frac{b}{a} \right),$$

where  $\zeta(a, b) = q - 1 - T^{\frac{q-1}{2}}(b) - T^{\frac{q-1}{2}}(ab)$ .

*Proof.* We follow the technique followed by Fusilier [14] and Lennon [27] to prove the theorem. Let

$$P(x, y) = ax^2 + y^2 - 1 - bx^2y^2.$$

Then

$$\#C_{a,b}(\mathbb{F}_q) = \#\{(x, y) \in \mathbb{F}_q^2 : P(x, y) = 0\}.$$

Using the elementary identity (2.2.3) deduced from (1.3.1), we obtain

$$\begin{aligned} q \cdot \#C_{a,b}(\mathbb{F}_q) &= \sum_{x,y,z \in \mathbb{F}_q} \theta(zP(x, y)) \\ &= q^2 + \sum_{z \in \mathbb{F}_q^\times} \theta(-z) + \sum_{x,z \in \mathbb{F}_q^\times} \theta(-z)\theta(za^2x^2) + \sum_{y,z \in \mathbb{F}_q^\times} \theta(-z)\theta(zy^2) \\ &\quad + \sum_{x,y,z \in \mathbb{F}_q^\times} \theta(zP(x, y)) \\ &:= q^2 + A + B + C + D. \end{aligned} \tag{2.3.1}$$

We use Lemma 1.3.11 and Lemma 1.3.7 repeatedly to each term of (2.3.1) to simplify the expression. First, we obtain that

$$A = \frac{1}{q-1} \sum_{l=0}^{q-2} G_{-l} T^l(-1) \sum_{z \in \mathbb{F}_q^\times} T^l(z) = -1.$$

Expanding the next term yields

$$B = \frac{1}{(q-1)^2} \sum_{l,m=0}^{q-2} G_{-l} G_{-m} T^l(-1) T^m(a) \sum_{z \in \mathbb{F}_q^\times} T^{l+m}(z) \sum_{x \in \mathbb{F}_q^\times} T^{2m}(x),$$

which is nonzero when  $l = -m$  and  $m = 0$  or  $\frac{q-1}{2}$ . Using this and Lemma 1.3.7, we deduce that

$$B = 1 + G_{\frac{q-1}{2}} G_{-\frac{q-1}{2}} T^{\frac{q-1}{2}}(-a) = 1 + q T^{\frac{q-1}{2}}(a).$$

Similarly, we deduce that

$$C = \frac{1}{(q-1)^2} \sum_{l,m=0}^{q-2} G_{-l} G_{-m} T^l(-1) \sum_{z \in \mathbb{F}_q^\times} T^{l+m}(z) \sum_{y \in \mathbb{F}_q^\times} T^{2m}(y) = 1 + q.$$

Finally,

$$D = \frac{1}{(q-1)^4} \sum_{l,m,n,k=0}^{q-2} G_{-l} G_{-m} G_{-n} G_{-k} T^l(a) T^m(-1) T^k(-b) \times \\ \sum_{z \in \mathbb{F}_q^\times} T^{l+m+n+k}(z) \sum_{x \in \mathbb{F}_q^\times} T^{2l+2k}(x) \sum_{y \in \mathbb{F}_q^\times} T^{2m+2k}(y).$$

Now,  $D$  will be nonzero only for the following four cases.

**Case 1.**  $l = -k, m = -k, n = k$ .

Using Lemma 1.3.10, we obtain

$$\begin{aligned} \frac{1}{q-1} \sum_{k=0}^{q-2} G_k G_{-k} G_k G_{-k} T^k(b/a) &= \frac{1}{q-1} \left\{ 1 + q^2 \sum_{k=1}^{q-2} T^k(b/a) \right\} \\ &= \frac{1 - q^2}{q-1} \\ &= -(1+q). \end{aligned}$$

**Case 2.**  $l = -k + \frac{q-1}{2}, m = -k, n = k - \frac{q-1}{2}$ .

Here, we use Lemma 1.3.12 and then Lemma 1.3.16 to deduce

$$\begin{aligned}
& \frac{1}{q-1} \sum_{k=0}^{q-2} G_{k-\frac{q-1}{2}} G_{-k} G_k G_{-k+\frac{q-1}{2}} T^{\frac{q-1}{2}}(-a) T^k(b/a) \\
&= \frac{q^2}{q-1} \sum_{k=0}^{q-2} G_{\frac{q-1}{2}}^2 \begin{pmatrix} T^{k-\frac{q-1}{2}} \\ T^k \end{pmatrix} \begin{pmatrix} T^k \\ T^{k-\frac{q-1}{2}} \end{pmatrix} T^{\frac{q-1}{2}}(a) T^k(b/a) \\
&= q^2 T^{\frac{q-1}{2}}(-a) {}_2F_1 \left( \begin{matrix} T^{\frac{q-1}{2}}, & \varepsilon \\ & T^{\frac{q-1}{2}} \end{matrix} \middle| \frac{b}{a} \right) \\
&= -q T^{\frac{q-1}{2}}(b) - q T^{\frac{q-1}{2}}(a).
\end{aligned}$$

**Case 3.**  $l = -k, m = -k + \frac{q-1}{2}, n = k - \frac{q-1}{2}$ .

As in case 2, we obtain

$$\begin{aligned}
& \frac{1}{q-1} \sum_{k=0}^{q-2} G_{k-\frac{q-1}{2}} G_{-k} G_k G_{-k+\frac{q-1}{2}} T^{\frac{q-1}{2}}(-1) T^k(b/a) \\
&= q^2 T^{\frac{q-1}{2}}(-1) {}_2F_1 \left( \begin{matrix} T^{\frac{q-1}{2}}, & \varepsilon \\ & T^{\frac{q-1}{2}} \end{matrix} \middle| \frac{b}{a} \right) \\
&= -q T^{\frac{q-1}{2}}(b/a) - q \\
&= -q T^{\frac{q-1}{2}}(ab) - q.
\end{aligned}$$

**Case 4.**  $l = -k + \frac{q-1}{2}, m = -k + \frac{q-1}{2}, n = k$ .

In this case, Lemma 1.3.12 yields

$$\begin{aligned}
& \frac{1}{q-1} \sum_{k=0}^{q-2} G_{k-\frac{q-1}{2}} G_{-k} G_{k-\frac{q-1}{2}} G_{-k} T^{\frac{q-1}{2}}(a) T^k(b/a) \\
&= \frac{q^2}{q-1} \sum_{k=0}^{q-2} G_{\frac{q-1}{2}}^2 \begin{pmatrix} T^{k-\frac{q-1}{2}} \\ T^k \end{pmatrix} \begin{pmatrix} T^{k-\frac{q-1}{2}} \\ T^k \end{pmatrix} T^{\frac{q-1}{2}}(a) T^k(b/a) \\
&= q^2 T^{\frac{q-1}{2}}(-a) {}_2F_1 \left( \begin{matrix} T^{\frac{q-1}{2}}, & T^{\frac{q-1}{2}} \\ & \varepsilon \end{matrix} \middle| \frac{b}{a} \right).
\end{aligned}$$

Combining all the terms together in (2.3.1), we obtain

$$q \cdot \#C_{a,b}(\mathbb{F}_q) = q^2 - q - qT^{\frac{q-1}{2}}(b) - qT^{\frac{q-1}{2}}(ab) + q^2T^{\frac{q-1}{2}}(-a) {}_2F_1 \left( \begin{matrix} T^{\frac{q-1}{2}}, & T^{\frac{q-1}{2}} \\ \varepsilon & \left| \frac{b}{a} \right. \end{matrix} \right),$$

which completes the proof.  $\square$

The Edward family of elliptic curves is birationally equivalent to the elliptic curve  $E_{\alpha\beta,\beta^2,0}$ . It is to be noted that  $E_{\alpha\beta,\beta^2,0}$  contains more families of elliptic curves including the Legendre's family.

**Theorem 2.3.2.** *Let  $q = p^e$ ,  $p > 0$ , be an odd prime. If  $\alpha \neq \pm 2$  and  $\beta \neq 0$ , then the trace of Frobenius on the elliptic curve  $E_{\alpha\beta,\beta^2,0}$  can be expressed as*

$$a_q(E_{\alpha\beta,\beta^2,0}) = -q\phi(-\alpha\beta - 2\beta) {}_2F_1 \left( \begin{matrix} \phi, & \phi \\ \varepsilon & \left| \frac{\alpha - 2}{\alpha + 2} \right. \end{matrix} \right).$$

*Proof.* Consider the elliptic curve

$$E_{\alpha\beta,\beta^2,0} : y^2 = x^3 + \alpha\beta x^2 + \beta^2 x.$$

Following [7], we perform the birational change of variables  $x \rightarrow \frac{\beta x}{y}$ ,  $y \rightarrow \frac{\beta(x-1)}{(x+1)}$  to obtain the equivalent form  $C_{a,b}$  as

$$C_{a,b} : ax^2 + y^2 = 1 + bx^2y^2,$$

where  $a = \alpha\beta + 2\beta$  and  $b = \alpha\beta - 2\beta$ . Now, the points on  $E_{\alpha\beta,\beta^2,0}$  for  $y = 0$  and  $x = -1$  do not correspond to any point on  $C_{a,b}$ .

1. For  $y = 0$ , there are  $2 + T^{\frac{q-1}{2}}(\alpha^2 - 4)$  extra points on  $E_{\alpha\beta,\beta^2,0}$ .
2. Also  $x = -1$  corresponds  $1 + T^{\frac{q-1}{2}}(\alpha\beta - 2\beta)$  extra points on  $E_{\alpha\beta,\beta^2,0}$ .

Similarly, under the inverse transformation  $x \rightarrow \frac{\beta(1+y)}{(1-y)}$ ,  $y \rightarrow \frac{\beta(1+y)}{x(1-y)}$ , the twisted Edward curve  $C_{a,b}$  is birationally equivalent to  $E_{\alpha\beta,\beta^2,0}$ . Again, the points on  $C_{a,b}$

for  $y = 1$  and  $x = 0$  do not correspond to any point on  $E_{\alpha\beta,\beta^2,0}$ . In this case,  $(0, 1)$  and  $(0, -1)$  are the only extra points on  $C_{a,b}$ . Hence, considering all we have

$$\#E_{\alpha\beta,\beta^2,0} = \#C_{a,b} + T^{\frac{q-1}{2}}(\alpha^2 - 4) + T^{\frac{q-1}{2}}(\alpha\beta - 2\beta) + 2$$

Thus, Theorem 2.3.1 and the fact  $a_q(E_{\alpha\beta,\beta^2,0}) = 1 + q - \#E_{\alpha\beta,\beta^2,0}(\mathbb{F}_q)$ , together complete the proof.  $\square$

**Corollary 2.3.3.** *Let  $q = p^e$ ,  $p > 0$ , be an odd prime and  $q \equiv 1 \pmod{4}$ . If  $\alpha\beta \neq 0$  and  $\alpha \neq \pm 2$ , then*

$${}_2F_1 \left( \begin{matrix} T^{\frac{q-1}{4}}, & T^{\frac{3(q-1)}{4}} \\ & \varepsilon \end{matrix} \middle| \frac{4}{\alpha^2} \right) = T^{\frac{q-1}{4}}(-1)\phi(2\alpha^2 + 4\alpha){}_2F_1 \left( \begin{matrix} \phi, & \phi \\ & \varepsilon \end{matrix} \middle| \frac{\alpha - 2}{\alpha + 2} \right).$$

*Proof.* Replacing  $f = \alpha\beta$  and  $g = \beta^2$  in Theorem 2.2.4, we have

$$a_q(E_{\alpha\beta,\beta^2,0}) = -qT^{\frac{q-1}{4}}(-1)\phi(2\alpha\beta){}_2F_1 \left( \begin{matrix} T^{\frac{q-1}{4}}, & T^{\frac{3(q-1)}{4}} \\ & \varepsilon \end{matrix} \middle| \frac{4}{\alpha^2} \right).$$

Then combining this with Theorem 2.3.2 we complete the proof.  $\square$

# Chapter 3

## Hypergeometric Functions and

$$y^\ell = x(x-1)(x-\lambda)$$

### 3.1 Introduction

Recall that every elliptic curve  $E$  over  $\mathbb{C}$  can be written in the Weierstrass normal form

$$y^2 = 4x^3 - g_2x - g_3, \quad (3.1.1)$$

with  $g_2, g_3 \in \mathbb{C}$ . If  $E(\mathbb{C})$  denotes the group of complex points on  $E$ , then we can associate a period lattice  $\Lambda$  to  $E$  via the biholomorphic mapping  $\varphi : \mathbb{C}/\Lambda \rightarrow E(\mathbb{C})$  given by

$$\varphi(z) = \begin{cases} [\wp(z) : \wp'(z) : 1], & \text{for } z \notin \Lambda; \\ [0 : 1 : 0], & \text{for } z \in \Lambda, \end{cases}$$

where  $\wp$  is the Weierstrass  $\wp$ -function. If  $g_2, g_3 \in \mathbb{R}$  then  $\Lambda$  can be chosen to be of the form  $\Lambda = \Omega(E)\mathbb{Z} + \Omega'(E)\mathbb{Z}$ , where  $\Omega(E) \in \mathbb{R}$  and  $\Omega'(E) \in \mathbb{C}$ . We call  $\Omega(E)$  the real period of  $E$ . Furthermore, if the right-hand side of (3.1.1) has three real roots then  $\Omega'(E)$  will be strictly imaginary. Thus, the period of an elliptic curve is a characterization to the real points of order 2 on the curve.

In this chapter, we define  $\Omega(C_{\ell,\lambda})$  for an algebraic curve  $C_{\ell,\lambda}$  of degree  $\ell$  analogous to the real period of elliptic curves and find a relation with ordinary hypergeometric

---

<sup>2</sup>The contents of this chapter have been published in *The Ramanujan J.* (2012).

series. We also give a relation between the number of points on  $C_{\ell,\lambda}$  over a finite field and Gaussian hypergeometric series. Finally, we give an alternate proof of a result of [36] and develop the interplay between binomial coefficients involving rational numbers and those involving multiplicative characters by providing some expressions for  $a_p(C_{\ell,\lambda})$  and  $\Omega(C_{\ell,\lambda})$ .

## 3.2 Main results

Let  $\lambda \in \mathbb{Q} \setminus \{0, 1\}$  and  $\ell \geq 2$ , and denote by  $C_{\ell,\lambda}$  the nonsingular projective curve over  $\mathbb{Q}$  with affine equation given by

$$y^\ell = x(x-1)(x-\lambda). \quad (3.2.1)$$

The change of variables  $(x, y) \mapsto (x + \frac{1+\lambda}{3}, \frac{y}{2})$  takes (3.2.1) to

$$y^\ell = 2^\ell(x-a)(x-b)(x-c), \quad (3.2.2)$$

where  $a = -\frac{1+\lambda}{3}$ ,  $b = \frac{2\lambda-1}{3}$ , and  $c = \frac{2-\lambda}{3}$ .

**Remark 3.2.1.** *If  $\ell = 3$ ,  $C_{\ell,\lambda}$  is an elliptic curve. Dehomogenizing the projective curve  $C_{3,\lambda} : Y^3 = X(X-Z)(X-\lambda Z)$  by putting  $X = 1$  and then making the substitution*

$$Y \rightarrow \lambda x, Z \rightarrow \lambda \left( y + \frac{1+\lambda}{2\lambda^2} \right),$$

*we find that  $C_{3,\lambda}$  is isomorphic over  $\mathbb{Q}$  to the elliptic curve*

$$y^2 = x^3 + \left( \frac{\lambda-1}{2\lambda^2} \right)^2. \quad (3.2.3)$$

### 3.2.1 On $y^\ell = x(x-1)(x-\lambda)$ and classical hypergeometric series

We define an integral for the family of curves (3.2.1) analogous to the real period of elliptic curves.

**Definition 3.2.1.** The complex number  $\Omega(C_{\ell,\lambda})$  is defined as

$$\Omega(C_{\ell,\lambda}) := 2 \int_a^b \frac{dx}{y^{\ell-1}},$$

where  $x$  and  $y$  are related as in (3.2.2).

It is to be noted that,  $C_{2,\lambda}$  is the elliptic curve in Legendre normal form with real period  $\Omega(C_{2,\lambda})$ , and  $C_{3,\lambda}$  represents the elliptic curve (3.2.3) with period integral  $\Omega(C_{3,\lambda})$ . In the following theorem, we express the integral  $\Omega(C_{\ell,\lambda})$  in terms of  ${}_2F_1$  classical hypergeometric series.

**Theorem 3.2.1.** *If  $0 < \lambda < 1$ , then  $\Omega(C_{\ell,\lambda})$  is given by*

$$\Omega(C_{\ell,\lambda}) = \frac{(\Gamma(\frac{1}{\ell}))^2}{2^{\ell-2} \lambda^{\frac{\ell-2}{\ell}} \Gamma(\frac{2}{\ell})} \cdot {}_2F_1 \left( \begin{matrix} (\ell-1)/\ell, & 1/\ell \\ & 2/\ell \end{matrix} \middle| \lambda \right).$$

*Proof.* Recalling (3.2.2), from the definition of  $\Omega(C_{\ell,\lambda})$ , we have

$$\begin{aligned} \Omega(C_{\ell,\lambda}) &= 2 \int_a^b \frac{dx}{y^{\ell-1}} \\ &= 2 \int_a^b \frac{dx}{2^{\ell-1} \{(x-a)(x-b)(x-c)\}^{\frac{\ell-1}{\ell}}}. \end{aligned}$$

Note that  $a < x < b$  and  $0 < \lambda < 1$ . Hence  $(x-a)$  is positive, while  $(x-b)$  and  $(x-c)$  are negative. Thus  $\Omega(C_{\ell,\lambda})$  is real.

Putting  $(x-a) = (b-a) \sin^2 \theta$ , we obtain

$$\begin{aligned} \Omega(C_{\ell,\lambda}) &= 2 \int_0^{\pi/2} \frac{2(b-a) \sin \theta \cos \theta}{2^{\ell-1} [(b-a) \sin^2 \theta (b-a) \cos^2 \theta \{(c-a) - (b-a) \sin^2 \theta\}]^{\frac{\ell-1}{\ell}}} d\theta \\ &= \frac{1}{2^{\ell-3}} \int_0^{\pi/2} \frac{(b-a)^{\frac{2-\ell}{\ell}} (\sin \theta)^{\frac{2-\ell}{\ell}} (\cos \theta)^{\frac{2-\ell}{\ell}}}{\{(c-a) - (b-a) \sin^2 \theta\}^{\frac{\ell-1}{\ell}}} d\theta. \end{aligned}$$

Using  $(b-a) = \lambda$  and  $(c-a) = 1$  yields

$$\begin{aligned} \Omega(C_{\ell,\lambda}) &= \frac{1}{2^{\ell-3} \lambda^{\frac{\ell-2}{\ell}}} \int_0^{\pi/2} \frac{(\sin \theta)^{2\frac{1}{\ell}-1} (\cos \theta)^{2\frac{1}{\ell}-2\frac{1}{\ell}-1}}{(1 - \lambda \sin^2 \theta)^{\frac{\ell-1}{\ell}}} d\theta \\ &= \frac{(\Gamma(\frac{1}{\ell}))^2}{2^{\ell-2} \lambda^{\frac{\ell-2}{\ell}} \Gamma(\frac{2}{\ell})} \cdot {}_2F_1 \left( \begin{matrix} (\ell-1)/\ell, & 1/\ell \\ & 2/\ell \end{matrix} \middle| \lambda \right), \end{aligned}$$



where the last equality follows from Theorem 1.3.1. This completes the proof of the theorem.  $\square$

**Remark 3.2.2.** *If we put  $\ell = 2$  in Theorem 3.2.1, we obtain Theorem 1.2.1 using the facts that  $\Gamma(\frac{1}{2}) = \sqrt{\pi}$  and  $\Gamma(1) = 1$ .*

### 3.2.2 On $y^\ell = x(x-1)(x-\lambda)$ and Gaussian hypergeometric function

We define  $a_p(C_{\ell,\lambda})$  analogous to the trace of Frobenius of elliptic curves.

**Definition 3.2.2.** Suppose  $p$  is a prime of good reduction for  $C_{\ell,\lambda}$ . Define the integer  $a_p(C_{\ell,\lambda})$  by

$$a_p(C_{\ell,\lambda}) := 1 + p - \#C_{\ell,\lambda}(\mathbb{F}_p), \quad (3.2.4)$$

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

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

**Remark 3.2.3.** *For  $\lambda \neq 0, 1$ , we have*

$$C_{\ell,\lambda} : y^\ell = z^{\ell-3}x(x-z)(x-\lambda z). \quad (3.2.5)$$

Let  $\ell \geq 4$ , then  $z = 0$  implies that  $y^\ell = 0$ , and hence  $[1 : 0 : 0]$  is the only point at infinity. If  $\ell = 2$ , then for  $z = 0$ , we have  $x^3 = 0$ . Thus the point at infinity is  $[0 : 1 : 0]$ . Hence, if  $\ell \neq 3$ , then

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

Let  $\ell = 3$ . Putting  $z = 0$  in (3.2.5), we have  $y^3 = x^3$ . Let  $p \equiv 1 \pmod{3}$  and  $\omega \in \mathbb{F}_p^\times$  be of order 3. Then there are three points at infinity, namely,  $[1 : 1 : 0]$ ,  $[1 : \omega : 0]$ , and  $[1 : \omega^2 : 0]$ . Hence, in this case,

$$\#C_{\ell,\lambda}(\mathbb{F}_p) = 3 + \#\{(x, y) \in \mathbb{F}_p^2 : y^\ell = x(x-1)(x-\lambda)\}.$$

Again, if  $\ell = 3$  and  $p \equiv 2 \pmod{3}$ , then the point at infinity is  $[1 : 1 : 0]$ . Thus, in this case

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

With this notation, we have the following result which connects the number of points of  $C_{\ell,\lambda}$  over  $\mathbb{F}_p$  with Gaussian hypergeometric series.

**Theorem 3.2.2.** *If  $p \equiv 1 \pmod{\ell}$  and  $\text{ord}_p(\lambda(\lambda-1)) = 0$ , then  $a_p(C_{\ell,\lambda})$  satisfies*

$$-a_p(C_{\ell,\lambda}) = \begin{cases} p \cdot \sum_{i=1}^{\ell-1} \chi^i(-\lambda^2) {}_2F_1 \left( \begin{matrix} \bar{\chi}^i, & \chi^i \\ & \chi^{2i} \end{matrix} \middle| \lambda \right), & \text{if } \ell \neq 3; \\ 2 + p \cdot \sum_{i=1}^{\ell-1} \chi^i(-\lambda^2) {}_2F_1 \left( \begin{matrix} \bar{\chi}^i, & \chi^i \\ & \chi^{2i} \end{matrix} \middle| \lambda \right), & \text{if } \ell = 3, \end{cases}$$

where  $\chi$  is a character of  $\mathbb{F}_p$  of order  $\ell$ .

*Proof.* Since  $p \equiv 1 \pmod{\ell}$ , there exists a character  $\chi$  of order  $\ell$  on  $\mathbb{F}_p$ . Using (1.3.3), we have

$$\begin{aligned} & \sum_{i=1}^{\ell-1} \chi^i(-\lambda^2) {}_2F_1 \left( \begin{matrix} \bar{\chi}^i, & \chi^i \\ & \chi^{2i} \end{matrix} \middle| \lambda \right) \\ &= \sum_{i=1}^{\ell-1} \chi^i(-\lambda^2) \frac{\chi^i \chi^{2i}(-1)}{p} \sum_{t \in \mathbb{F}_p} \chi^i(t) \bar{\chi}^i \chi^{2i} (1-t) \bar{\chi}^i (1-\lambda t) \\ &= \sum_{i=1}^{\ell-1} \chi^i(-\lambda^2) \frac{\chi^{3i}(-1)}{p} \sum_{t \in \mathbb{F}_p} \chi^i(t) \chi^i(1-t) \chi^i(1-\lambda t). \end{aligned}$$

Replacing  $t$  by  $\frac{t}{\lambda}$ , we deduce

$$\begin{aligned} p \cdot \sum_{i=1}^{\ell-1} \chi^i(-\lambda^2) {}_2F_1 \left( \begin{matrix} \bar{\chi}^i, & \chi^i \\ & \chi^{2i} \end{matrix} \middle| \lambda \right) &= \sum_{i=1}^{\ell-1} \sum_{t \in \mathbb{F}_p} \chi^i(t(t-1)(t-\lambda)) \\ &= \sum_{t \in \mathbb{F}_p} \sum_{i=1}^{\ell-1} \chi^i(t(t-1)(t-\lambda)). \end{aligned} \quad (3.2.6)$$

Moreover,

$$\begin{aligned}
& \#\{(x, y) \in \mathbb{F}_p^2 : y^\ell = x(x-1)(x-\lambda)\} \\
&= \sum_{t \in \mathbb{F}_p} \#\{y \in \mathbb{F}_p : y^\ell = t(t-1)(t-\lambda)\} \\
&= \sum_{t \in \mathbb{F}_p, t(t-1)(t-\lambda) \neq 0} \#\{y \in \mathbb{F}_p : y^\ell = t(t-1)(t-\lambda)\} + \#\{t \in \mathbb{F}_p : t(t-1)(t-\lambda) = 0\}.
\end{aligned}$$

Now applying Lemma 1.3.6, we obtain

$$\begin{aligned}
& \#\{(x, y) \in \mathbb{F}_p^2 : y^\ell = x(x-1)(x-\lambda)\} \\
&= \sum_{t \in \mathbb{F}_p} \sum_{i=0}^{\ell-1} \chi^i(t(t-1)(t-\lambda)) + \#\{t \in \mathbb{F}_p : t(t-1)(t-\lambda) = 0\} \\
&= \left\{ \#\{t \in \mathbb{F}_p : t(t-1)(t-\lambda) = 0\} + \sum_{t \in \mathbb{F}_p} \varepsilon(t(t-1)(t-\lambda)) \right\} \\
&\quad + \sum_{t \in \mathbb{F}_p} \sum_{i=1}^{\ell-1} \chi^i(t(t-1)(t-\lambda)) \\
&= p + \sum_{t \in \mathbb{F}_p} \sum_{i=1}^{\ell-1} \chi^i(t(t-1)(t-\lambda)).
\end{aligned}$$

Then the equation (3.2.6) yields

$$\#\{(x, y) \in \mathbb{F}_p^2 : y^\ell = x(x-1)(x-\lambda)\} = p + p \cdot \sum_{i=1}^{\ell-1} \chi^i(-\lambda^2) {}_2F_1 \left( \begin{matrix} \overline{\chi^i}, & \chi^i \\ & \chi^{2i} \end{matrix} \mid \lambda \right).$$

Since  $\text{ord}_p(\lambda(\lambda-1)) = 0$ ; using (3.2.4) and Remark 3.2.3 we complete the proof of the result.  $\square$

**Remark 3.2.4.** *Theorem 1.2.3 (a) can be obtained from Theorem 3.2.2 by putting  $\ell = 2$ . Note that for the quadratic character  $\phi$  of  $\mathbb{F}_p$ , we have  $\phi(-\lambda^2) = \phi(-1)$ .*

**Remark 3.2.5.** *The formula for  $a_p(C_{3,\lambda})$  in Theorem 3.2.2 gives the trace of Frobenius of the family of elliptic curves (3.2.3).*

A typical result in the direction of finding the number of solutions over a finite field of a polynomial equation is the Hasse-Weil bound, which states that a smooth projective curve of genus  $g$  defined over a finite field with  $q$  elements has between  $q + 1 - 2g\sqrt{q}$  and  $q + 1 + 2g\sqrt{q}$  points. For  $\ell \geq 3$ , the genus of the curve  $C_{\ell,\lambda}$  is  $\frac{(\ell-1)(\ell-2)}{2}$ . Thus, the Hasse-Weil bound yields the following corollary.

**Corollary 3.2.3.** *Suppose  $\ell \geq 4$ . If  $p \equiv 1 \pmod{\ell}$  and  $\text{ord}_p(\lambda(\lambda - 1)) = 0$ , then*

$$\left| \sum_{i=1}^{\ell-1} \chi^i(-\lambda^2) {}_2F_1 \left( \begin{matrix} \bar{\chi}^i, & \chi^i \\ & \chi^{2i} \end{matrix} \middle| \lambda \right) \right| \leq \frac{(\ell-1)(\ell-2)}{\sqrt{p}},$$

where  $\chi$  is a character of  $\mathbb{F}_p$  of order  $\ell$ .

If  $\ell = 3$ , then

$$\left| 2 + p \cdot \sum_{i=1}^2 \chi^i(-\lambda^2) {}_2F_1 \left( \begin{matrix} \bar{\chi}^i, & \chi^i \\ & \chi^{2i} \end{matrix} \middle| \lambda \right) \right| \leq 2\sqrt{p},$$

where  $\chi$  is a character of  $\mathbb{F}_p$  of order 3.

**Corollary 3.2.4.** *If  $p \equiv 1 \pmod{3}$  and  $x^2 + 3y^2 = p$ , then*

$$p \cdot \sum_{i=1}^2 {}_2F_1 \left( \begin{matrix} \bar{\chi}^i, & \chi^i \\ & \chi^{2i} \end{matrix} \middle| -1 \right) = (-1)^{x+y} \left( \frac{x}{3} \right) \cdot 2x - 2,$$

where  $\chi$  is a character of  $\mathbb{F}_p$  of order 3.

*Proof.* As mentioned in Remark 3.2.1,  $C_{3,-1}$  is isomorphic over  $\mathbb{Q}$  to the elliptic curve

$$E : y^2 = x^3 + 1.$$

Therefore,

$$a_p(C_{3,-1}) = a_p(E). \quad (3.2.7)$$

Again, [34, Prop. 2] states that

$$a_p(E) = (-1)^{x+y-1} \left( \frac{x}{3} \right) \cdot 2x. \quad (3.2.8)$$

Using (3.2.8) in (3.2.7), the result follows from Theorem 3.2.2.  $\square$

### 3.3 Analog between classical and Gaussian hypergeometric series

Greene [18] introduced the notion of hypergeometric series over finite fields, which are analogous to the classical hypergeometric series. Since then, the interplay between ordinary hypergeometric series and Gaussian hypergeometric series has played an important role in character sum evaluation [20], the representation theory of  $SL(2, \mathbb{R})$  [19], finite field versions of the Lagrange inversion formula [21], and finding the number of points on an algebraic curve over finite fields [34]. Recently, Rouse [36] and McCarthy [30] provided expressions for the traces of Frobenius of certain families of elliptic curves in terms of Gaussian hypergeometric series. These formulas are analogous to the expressions for the real periods of the curves in terms of classical hypergeometric series. Moreover, the classical hypergeometric series expression of the period integral of  $C_{\ell, \lambda}$  given in Theorem 3.2.1 is analogous to the Gaussian hypergeometric series expression of the number of  $\mathbb{F}_p$ -points on  $C_{\ell, \lambda}$  given in Theorem 3.2.2. This section examines this analogy further and provides a striking analogy between binomial coefficients involving rational numbers and those involving multiplicative characters.

**Theorem 3.3.1.** *For  $\lambda = \frac{1}{2}$ , we have*

$$\frac{2^{\frac{(\ell-3)(\ell-1)}{\ell}} \Gamma(\frac{2}{\ell})}{(\Gamma(\frac{1}{\ell}))^2} \cdot \Omega(C_{\ell, \lambda}) = \frac{\binom{\frac{1}{2\ell}}{\frac{1}{\ell}}}{\binom{\frac{3-2\ell}{2\ell}}{\frac{2-\ell}{\ell}}}. \quad (3.3.1)$$

Moreover, if  $p \equiv 1 \pmod{\ell}$ , then

$$-a_p(C_{\ell, \frac{1}{2}}) = \begin{cases} p \cdot \sum_{i=1}^{\lfloor \frac{\ell-1}{2} \rfloor} \chi^{-2i}(8) \left[ \binom{\chi^i}{\chi^{-2i}} + \binom{\phi\chi^i}{\chi^{-2i}} \right], & \text{if } \frac{p-1}{\ell} \text{ is odd and } \ell \neq 3; \\ p \cdot \sum_{i=1}^{\ell-1} \chi^{-i}(8) \left[ \binom{\sqrt{\chi^i}}{\chi^{-i}} + \binom{\phi\sqrt{\chi^i}}{\chi^{-i}} \right], & \text{if } \frac{p-1}{\ell} \text{ is even and } \ell \neq 3; \\ 2 + p \cdot \sum_{i=1}^2 \left[ \binom{\sqrt{\chi^i}}{\chi^{-i}} + \binom{\phi\sqrt{\chi^i}}{\chi^{-i}} \right], & \text{if } \ell = 3, \end{cases} \quad (3.3.2)$$

where  $\chi$  is a character of  $\mathbb{F}_p$  of order  $\ell$  and  $\phi$  is the quadratic character.

*Proof.* By Theorem 1.3.4, we have

$$\begin{aligned} {}_2F_1 \left( \begin{matrix} (\ell-1)/\ell, & 1/\ell \\ & 2/\ell \end{matrix} \middle| -1 \right) &= \frac{\Gamma(\frac{2}{\ell})\Gamma(\frac{2\ell+1}{2\ell})}{\Gamma(\frac{\ell+1}{\ell})\Gamma(\frac{3}{2\ell})} \\ &= \frac{\Gamma(\frac{2\ell+1}{2\ell})}{\Gamma(\frac{\ell+1}{\ell})\Gamma(\frac{2\ell-1}{2\ell})} \\ &= \frac{\Gamma(\frac{3}{2\ell})}{\Gamma(\frac{2}{\ell})\Gamma(\frac{2\ell-1}{2\ell})} \\ &= \frac{\left(\frac{1}{2\ell}\right)}{\left(\frac{1}{\ell}\right)} \\ &= \frac{\left(\frac{3-2\ell}{2\ell}\right)}{\left(\frac{2-\ell}{\ell}\right)}. \end{aligned} \quad (3.3.3)$$

Putting  $\lambda = 1/2$  in Theorem 3.2.1, we obtain the relation

$$\frac{2^{\frac{\ell^2-3\ell+2}{\ell}}\Gamma(\frac{2}{\ell})}{(\Gamma(\frac{1}{\ell}))^2} \cdot \Omega(C_{\ell, \frac{1}{2}}) = {}_2F_1 \left( \begin{matrix} (\ell-1)/\ell, & 1/\ell \\ & 2/\ell \end{matrix} \middle| \frac{1}{2} \right).$$

Then using Theorem 1.3.2, we have

$${}_2F_1 \left( \begin{matrix} (\ell-1)/\ell, & 1/\ell \\ & 2/\ell \end{matrix} \middle| \frac{1}{2} \right) = 2^{\frac{\ell-1}{\ell}} {}_2F_1 \left( \begin{matrix} (\ell-1)/\ell, & 1/\ell \\ & 2/\ell \end{matrix} \middle| -1 \right).$$

Thus

$$\frac{2^{\frac{\ell^2-3\ell+2}{\ell}}\Gamma(\frac{2}{\ell})}{(\Gamma(\frac{1}{\ell}))^2} \cdot \Omega(C_{\ell, \frac{1}{2}}) = 2^{\frac{\ell-1}{\ell}} {}_2F_1 \left( \begin{matrix} (\ell-1)/\ell, & 1/\ell \\ & 2/\ell \end{matrix} \middle| -1 \right). \quad (3.3.4)$$

From (3.3.3) and (3.3.4), we complete the proof of (3.3.1).

Now, we shall prove the second part of the result. Putting  $\lambda = \frac{1}{2}$  in Theorem 3.2.2, we have

$$-a_p(C_{\ell, \frac{1}{2}}) = \begin{cases} p \cdot \sum_{i=1}^{\ell-1} \chi^i(-\frac{1}{4}) {}_2F_1 \left( \begin{matrix} \bar{\chi}^i, & \chi^i \\ & \chi^{2i} \end{matrix} \middle| \frac{1}{2} \right), & \text{if } \ell \neq 3; \\ 2 + p \cdot \sum_{i=1}^{\ell-1} \chi^i(-\frac{1}{4}) {}_2F_1 \left( \begin{matrix} \bar{\chi}^i, & \chi^i \\ & \chi^{2i} \end{matrix} \middle| \frac{1}{2} \right), & \text{if } \ell = 3. \end{cases} \quad (3.3.5)$$

Again, from [18, (4.15)], we have

$${}_2F_1 \left( \begin{matrix} A & \bar{A} \\ \bar{A}B & \end{matrix} \middle| \frac{1}{2} \right) = A(-2) \begin{cases} 0, & \text{if } B \text{ is not a square;} \\ \left[ \begin{matrix} (C) \\ (A) \end{matrix} \right] + \left( \begin{matrix} \phi C \\ A \end{matrix} \right), & \text{if } B = C^2. \end{cases}$$

Using this in (3.3.5), we obtain

$$-a_p(C_{\ell, \frac{1}{2}}) = \begin{cases} p \cdot \sum_{i=1}^{\lfloor \frac{\ell-1}{2} \rfloor} \chi^{-2i}(8) \left[ \begin{matrix} (\chi^i) \\ (\chi^{-2i}) \end{matrix} \right] + \left( \begin{matrix} \phi \chi^i \\ \chi^{-2i} \end{matrix} \right), & \text{if } \chi \text{ is not square and } \ell \neq 3; \\ p \cdot \sum_{i=1}^{\ell-1} \chi^{-i}(8) \left[ \begin{matrix} (\sqrt{\chi^i}) \\ (\chi^{-i}) \end{matrix} \right] + \left( \begin{matrix} \phi \sqrt{\chi^i} \\ \chi^{-i} \end{matrix} \right), & \text{if } \chi \text{ is square and } \ell \neq 3; \\ 2 + p \cdot \sum_{i=1}^2 \left[ \begin{matrix} (\sqrt{\chi^i}) \\ (\chi^{-i}) \end{matrix} \right] + \left( \begin{matrix} \phi \sqrt{\chi^i} \\ \chi^{-i} \end{matrix} \right), & \text{if } \ell = 3, \end{cases} \quad (3.3.6)$$

Note that  $p$  is an odd prime. Write  $\chi = w^k$ , where  $w$  is a generator of the group of Dirichlet characters mod  $p$ . Let  $o(w)$  denote the order of  $w$ . Then  $o(w) = p-1$  and  $\ell = o(w^k) = (p-1)/\gcd(k, p-1)$ . So  $(p-1)/\ell = \gcd(k, p-1)$ .

If  $(p-1)/\ell$  is even, then  $k$  is also even, hence  $\chi$  is a square.

Conversely, if  $\chi$  is a square, it is an even power of the generator  $w$ , hence  $k$  is even, and  $(p-1)/\ell = \gcd(k, p-1)$  is even.

This implies that  $\chi$  is a square if and only if  $(p-1)/\ell$  is even. Moreover,  $\chi^i$  is always a square for even values of  $i$ , and for odd values of  $i$ ,  $\chi^i$  is a square if and only if  $\chi$  is a square. Using these, from (3.3.6), we complete the proof of (3.3.2).  $\square$

In [36], Rouse gave an analogy between ordinary hypergeometric series and Gaussian hypergeometric series by evaluating  $\Omega(C_{2,\frac{1}{2}})$  and  $a_p(C_{2,\frac{1}{2}})$  in terms of hypergeometric series. We now give an alternate proof of [36, Thm. 3, p. 3] with the note that  $\binom{1/4}{1/2}$  is real. Here we extend the definition of binomial coefficient to include rational arguments via

$$\binom{n}{k} = \frac{\Gamma(n+1)}{\Gamma(k+1)\Gamma(n-k+1)}.$$

The statement of the result is as follow.

**Theorem 3.3.2.** [36, Thm. 3] *If  $\lambda = 1/2$ , then*

$$\frac{\sqrt{2}}{2\pi} \cdot \Omega(C_{2,\lambda}) = \binom{1/4}{1/2}.$$

*If  $p \equiv 1 \pmod{4}$ , then*

$$\frac{-\phi(-2)}{2p} \cdot a_p(C_{2,\lambda}) = \operatorname{Re} \left( \frac{\chi_4}{\phi} \right),$$

*where  $\chi_4$  is a character on  $\mathbb{F}_p$  of order 4 and  $\phi$  is the quadratic character.*

*Proof.* Putting  $\ell = 2$  in (3.3.1), we obtain

$$\frac{2^{-\frac{1}{2}}}{(\Gamma(\frac{1}{2}))^2} \cdot \Omega(C_{2,\frac{1}{2}}) = \frac{\binom{1/4}{1/2}}{\binom{-1/4}{0}}$$

which yields

$$\frac{\sqrt{2}}{2\pi} \cdot \Omega(C_{2,\frac{1}{2}}) = \binom{1/4}{1/2},$$

since  $\binom{-1/4}{0} = 1$  and  $\Gamma(\frac{1}{2}) = \sqrt{\pi}$ .

For the second part, recall that  $p \equiv 1 \pmod{4}$ . Putting  $\ell = 2$  in (3.3.2), we find that

$$\frac{-\phi(8)}{p} \cdot a_p(C_{2,\frac{1}{2}}) = \binom{\chi_4}{\phi} + \binom{\phi\chi_4}{\phi},$$



since  $\chi_4^2 = \phi$ . Clearly  $\phi\chi_4 = \overline{\chi_4}$ , and this implies that  $\begin{pmatrix} \phi\chi_4 \\ \phi \end{pmatrix} = \overline{\begin{pmatrix} \chi_4 \\ \phi \end{pmatrix}}$ . Also, observing that  $\phi(8) = \phi(2)$ , we obtain

$$\frac{-\phi(2)}{2p} \cdot a_p(C_{2, \frac{1}{2}}) = \operatorname{Re} \begin{pmatrix} \chi_4 \\ \phi \end{pmatrix}.$$

Since  $p \equiv 1 \pmod{4}$ , we have that  $\phi(-1) = 1$ , and hence the result follows.  $\square$

Simplifying the expressions for  $a_p(C_{\ell, \frac{1}{2}})$  given in (3.3.2), we obtain the following result which generalizes the case  $\ell = 2$ ,  $p \equiv 1 \pmod{4}$  treated in Theorem 3.3.2.

**Corollary 3.3.3.** *Suppose that  $p \equiv 1 \pmod{\ell}$ . Then we have*

$$-a_p(C_{\ell, \frac{1}{2}}) = \begin{cases} 2p \cdot \left[ \phi(2) \operatorname{Re} \begin{pmatrix} \chi_4 \\ \phi \end{pmatrix} + \sum_{i=1}^{\frac{\ell-4}{4}} \operatorname{Re} \left\{ \chi^{-2i}(8) \left( \begin{pmatrix} \chi^i \\ \chi^{-2i} \end{pmatrix} + \begin{pmatrix} \phi\chi^i \\ \chi^{-2i} \end{pmatrix} \right) \right\} \right], & \text{if } \frac{p-1}{\ell} \text{ is odd and } \ell \equiv 0 \pmod{4}; \\ 2p \cdot \sum_{i=1}^{\frac{\ell-2}{4}} \operatorname{Re} \left[ \chi^{-2i}(8) \left( \begin{pmatrix} \chi^i \\ \chi^{-2i} \end{pmatrix} + \begin{pmatrix} \phi\chi^i \\ \chi^{-2i} \end{pmatrix} \right) \right], & \text{if } \frac{p-1}{\ell} \text{ is odd and } \ell \equiv 2 \pmod{4}; \\ 2p \cdot \left[ \phi(2) \operatorname{Re} \begin{pmatrix} \chi_4 \\ \phi \end{pmatrix} + \sum_{i=1}^{\frac{\ell-2}{2}} \operatorname{Re} \left\{ \psi^{-2i}(8) \left( \begin{pmatrix} \psi^i \\ \psi^{-2i} \end{pmatrix} + \begin{pmatrix} \phi\psi^i \\ \psi^{-2i} \end{pmatrix} \right) \right\} \right], & \text{if } \frac{p-1}{\ell} \text{ and } \ell \text{ are even}; \\ 2p \cdot \sum_{i=1}^{\frac{\ell-1}{2}} \operatorname{Re} \left[ \psi^{-2i}(8) \left( \begin{pmatrix} \psi^i \\ \psi^{-2i} \end{pmatrix} + \begin{pmatrix} \phi\psi^i \\ \psi^{-2i} \end{pmatrix} \right) \right], & \text{if } \frac{p-1}{\ell} \text{ is even and } \ell \text{ is odd, } \ell \geq 5; \\ 2 + 2p \cdot \operatorname{Re} \left[ \begin{pmatrix} \chi \\ \chi \end{pmatrix} + \begin{pmatrix} \phi\chi \\ \chi \end{pmatrix} \right], & \text{if } \ell = 3; \end{cases}$$

where  $\psi, \chi, \chi_4$  are characters of  $\mathbb{F}_p$  of order  $2\ell, \ell, 4$  respectively and  $\phi$  is the quadratic character.

*Proof.* Let  $\chi$  be any character of order  $\ell$ . For each  $i$ , we have  $\chi^{\ell-i} = \overline{\chi^i}$  and

$\sqrt{\chi^{\ell-i}} = \sqrt{\chi^i}$ . Hence

$$\begin{aligned} \chi^{-2(\ell-i)}(8) \left[ \binom{\chi^{\ell-i}}{\chi^{-2(\ell-i)}} + \binom{\phi\chi^{\ell-i}}{\chi^{-2(\ell-i)}} \right] &= \chi^{2i}(8) \left[ \binom{\chi^{-i}}{\chi^{2i}} + \binom{\phi\chi^{-i}}{\chi^{2i}} \right] \\ &= \chi^{-2i}(8) \left[ \binom{\chi^i}{\chi^{-2i}} + \binom{\phi\chi^i}{\chi^{-2i}} \right] \end{aligned}$$

Thus, we have

$$\begin{aligned} \chi^{-2i}(8) \left[ \binom{\chi^i}{\chi^{-2i}} + \binom{\phi\chi^i}{\chi^{-2i}} \right] &+ \chi^{-2(\ell-i)}(8) \left[ \binom{\chi^{\ell-i}}{\chi^{-2(\ell-i)}} + \binom{\phi\chi^{\ell-i}}{\chi^{-2(\ell-i)}} \right] \\ &= 2\operatorname{Re} \left\{ \chi^{-2i}(8) \left[ \binom{\chi^i}{\chi^{-2i}} + \binom{\phi\chi^i}{\chi^{-2i}} \right] \right\} \end{aligned}$$

Therefore, the result follows from (3.3.2).  $\square$

**Corollary 3.3.4.** *If  $p \equiv 1 \pmod{3}$  and  $x^2 + 3y^2 = p$ , then*

$$p \cdot \operatorname{Re} \left[ \binom{\chi}{\chi} + \binom{\phi\chi}{\chi} \right] = (-1)^{x+y} \left( \frac{x}{3} \right) \cdot x - 1,$$

where  $\chi$  is a character of order 3 on  $\mathbb{F}_p$  and  $\phi$  is the quadratic character.

*Proof.* As mentioned in Remark 3.2.1,  $C_{3,-1}$  and  $C_{3,\frac{1}{2}}$  are isomorphic over  $\mathbb{Q}$  to the elliptic curve

$$y^2 = x^3 + 1.$$

From (3.2.7) and (3.2.8), it is known that

$$a_p(C_{3,-1}) = (-1)^{x+y-1} \left( \frac{x}{3} \right) \cdot 2x.$$

From Corollary 3.3.3, we have

$$-a_p(C_{3,\frac{1}{2}}) = 2 + 2p \cdot \operatorname{Re} \left[ \binom{\chi}{\chi} + \binom{\phi\chi}{\chi} \right].$$

Since  $a_p(C_{3,-1}) = a_p(C_{3,\frac{1}{2}})$ , the result follows.  $\square$

# 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

<sup>3</sup>The contents of this chapter have appeared in *Int. J. Number Theory* (2012).

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  $A, B \in \widehat{\mathbb{F}}_q^\times$  the function  $F(A, B; x)$  is defined by

$$F(A, B; x) := \frac{q}{q-1} \sum_x \binom{A\chi^2}{\chi} \binom{A\chi}{B\chi} \chi \left( \frac{x}{4} \right), \quad (4.2.1)$$

and its normalization as

$$F^*(A, B; x) := F(A, B; x) + AB(-1) \frac{\overline{A}(\frac{x}{4})}{q}. \quad (4.2.2)$$

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

$$g(A, B; x) := \sum_{t \in \mathbb{F}_q} A(1-t)B(1-xt^2), \quad x \in \mathbb{F}_q. \quad (4.2.3)$$

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*

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

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*

$${}_3F_2 \left( \begin{matrix} A, \overline{A}C^2, C\phi \\ C^2, C \end{matrix} \middle| x \right) = -\frac{\overline{C}(x)\phi(1-x)}{q} + C(-1)A\overline{C}(4)A\overline{C}^2(1-x) \times \\ \frac{J(\overline{A}C^2, A\overline{C})}{q^2 J(A, \overline{A}C)} \cdot g(A\overline{C}^2, \overline{A}C; 1-x)^2.$$

**Theorem 4.2.3.** [12, Thm. 1.2] *Let  $R^2 \notin \{\varepsilon, C, C^2\}$ . Then*

$$F^*(R^2, C; x) = R(4) \frac{J(\phi, C\bar{R}^2)}{J(\bar{R}C, \bar{R}\phi)} \cdot {}_2F_1 \left( \begin{matrix} R\phi, & R \\ & C \end{matrix} \middle| x \right).$$

We now prove a result similar to the above theorem.

**Proposition 4.2.4.** *We have*

$$F^*(\varepsilon, C; x) = \begin{cases} {}_2F_1 \left( \begin{matrix} \phi, & \varepsilon \\ & C \end{matrix} \middle| x \right), & \text{if } C \neq \varepsilon; \\ -(q-2) \cdot {}_2F_1 \left( \begin{matrix} \phi, & \varepsilon \\ & C \end{matrix} \middle| x \right), & \text{if } C = \varepsilon. \end{cases}$$

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

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

Putting  $B = \varepsilon$ , we have

$$\begin{pmatrix} \chi^2 \\ \chi \end{pmatrix} = \begin{pmatrix} \phi\chi \\ \chi \end{pmatrix} \begin{pmatrix} \chi \\ \chi \end{pmatrix} \begin{pmatrix} \phi \\ \phi \end{pmatrix}^{-1} \chi(4). \quad (4.2.4)$$

From (4.2.4) and (4.2.1), we obtain

$$\begin{aligned} F(\varepsilon, C; x) &= \frac{q}{q-1} \sum_x \begin{pmatrix} \chi^2 \\ \chi \end{pmatrix} \begin{pmatrix} \chi \\ C\chi \end{pmatrix} \chi \left( \frac{x}{4} \right) \\ &= \frac{q}{q-1} \sum_x \begin{pmatrix} \chi \\ C\chi \end{pmatrix} \begin{pmatrix} \phi\chi \\ \chi \end{pmatrix} \begin{pmatrix} \chi \\ \chi \end{pmatrix} \begin{pmatrix} \phi \\ \phi \end{pmatrix}^{-1} \chi(4) \chi \left( \frac{x}{4} \right) \\ &= \begin{pmatrix} \phi \\ \phi \end{pmatrix}^{-1} {}_3F_2 \left( \begin{matrix} \phi, & \varepsilon, & \varepsilon \\ & C, & \varepsilon \end{matrix} \middle| x \right). \end{aligned} \quad (4.2.5)$$

By Theorem 1.3.13, (4.2.5) reduces to

$$\begin{pmatrix} \phi \\ \phi \end{pmatrix} F(\varepsilon, C; x) = \begin{pmatrix} C \\ C \end{pmatrix} {}_2F_1 \left( \begin{matrix} \phi, & \varepsilon \\ & C \end{matrix} \middle| x \right) - \frac{C(-1)}{q} \begin{pmatrix} \phi \\ \varepsilon \end{pmatrix}. \quad (4.2.6)$$

From (4.2.2), we have

$$\begin{pmatrix} \phi \\ \phi \end{pmatrix} F(\varepsilon, C; x) = \begin{pmatrix} \phi \\ \phi \end{pmatrix} F^*(\varepsilon, C; x) - \frac{C(-1)}{q} \begin{pmatrix} \phi \\ \phi \end{pmatrix}. \quad (4.2.7)$$

Comparing equations (4.2.6) and (4.2.7), we obtain

$$F^*(\varepsilon, C; x) = \begin{pmatrix} C \\ C \end{pmatrix} \begin{pmatrix} \phi \\ \phi \end{pmatrix}^{-1} {}_2F_1 \left( \begin{matrix} \phi, & \varepsilon \\ & C \end{matrix} \middle| x \right).$$

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

### 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

$$y^\ell = (x-1)(x^2 + \lambda). \quad (4.3.1)$$

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

$$X - Z \rightarrow X, \quad Y \rightarrow Y \quad \text{and} \quad X \rightarrow X$$

*transforms the projective curve*

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

*to*

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

*Now dehomogenizing (4.3.2) by putting  $X = 1$  and then making the substitution*

$$Y \rightarrow (1 + \lambda)x, \quad Z \rightarrow (1 + \lambda)y - \frac{1}{1 + \lambda},$$

*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

$$\#V_{\ell,\lambda}(\mathbb{F}_q) = 1 + \#\{(x, y) \in \mathbb{F}_q^2 : y^\ell = (x - 1)(x^2 + \lambda)\}. \quad (4.3.3)$$

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,

$$\#V_{\ell,\lambda}(\mathbb{F}_q) = 3 + \#\{(x, y) \in \mathbb{F}_q^2 : y^\ell = (x - 1)(x^2 + \lambda)\}. \quad (4.3.4)$$

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

$${}_3F_2 \left( \begin{matrix} \phi, & \phi, & \phi \\ \varepsilon, & \varepsilon & \end{matrix} \middle| \frac{1+\lambda}{\lambda} \right) = \frac{\phi(-\lambda)(a_p(V_{2,\lambda})^2 - p)}{p^2}. \quad (4.3.5)$$

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*

$$\begin{aligned} a_q(V_{\ell,\lambda})^2 &= q^2 \cdot \sum_{i=1}^{\ell-1} \frac{J(S^{3i}, S^{-i})}{S^i(-4\lambda^3)J(S^i, S^i)} \cdot {}_3F_2 \left( \begin{matrix} S^{3i}, & S^i, & S^{2i}\phi \\ S^{4i}, & S^{2i} & \end{matrix} \middle| \frac{1+\lambda}{\lambda} \right) \\ &\quad + q \cdot \sum_{i=1}^{\ell-1} \frac{\phi(-\lambda)J(S^{3i}, S^{-i})}{S^i(-4\lambda(1+\lambda)^2)J(S^i, S^i)} + Q, \end{aligned}$$

where

$$Q = \begin{cases} (\ell-1)(q-1) - (\ell-3)a_q(V_{\ell,\lambda}), & \text{if } \ell \text{ is odd;} \\ (\ell-2)(q-1) - (\ell-2)a_q(V_{\ell,\lambda}) \\ -2q \cdot \sum_{i=1}^{\frac{\ell}{2}-1} \frac{J(\phi, S^{-2i})}{J(S^i\phi, S^{-3i})} \cdot {}_2F_1 \left( \begin{matrix} S^{3i}, & S^{3i}\phi \\ S^{4i} & \end{matrix} \middle| 1+\lambda \right), & \text{if } \ell \text{ is even} \end{cases}$$

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

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



which gives

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

Moreover,

$$\begin{aligned} & \#\{(x, y) \in \mathbb{F}_q^2 : y^\ell = (x-1)(x^2+\lambda)\} \\ &= \sum_{t \in \mathbb{F}_q} \#\{y \in \mathbb{F}_q : y^\ell = (t-1)(t^2+\lambda)\} \\ &= \sum_{t \in \mathbb{F}_q, (t-1)(t^2+\lambda) \neq 0} \#\{y \in \mathbb{F}_q : y^\ell = (t-1)(t^2+\lambda)\} + \#\{t \in \mathbb{F}_q : (t-1)(t^2+\lambda) = 0\}. \end{aligned}$$

Applying Lemma 1.3.6, we obtain

$$\begin{aligned} & \#\{(x, y) \in \mathbb{F}_q^2 : y^\ell = (x-1)(x^2+\lambda)\} \\ &= \sum_{t \in \mathbb{F}_q} \sum_{i=0}^{\ell-1} S^i((t-1)(t^2+\lambda)) + \#\{t \in \mathbb{F}_q : (t-1)(t^2+\lambda) = 0\} \\ &= q + \sum_{t \in \mathbb{F}_q} \sum_{i=1}^{\ell-1} S^i((t-1)(t^2+\lambda)). \end{aligned}$$

Since  $\text{ord}_p(\lambda(\lambda+1)) = 0$ , (4.3.3) yields

$$-a_q(V_{\ell, \lambda}) = \sum_{i=1}^{\ell-1} \sum_{t \in \mathbb{F}_q} S^i((t-1)(t^2+\lambda)). \quad (4.3.7)$$

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

$$\begin{aligned} a_q(V_{\ell, \lambda})^2 &= \sum_{i=1}^{\ell-1} S^i(\lambda^2)g\left(S^i, S^i; -\frac{1}{\lambda}\right)^2 + \sum_{i, j=1, i \neq j, i+j=\ell}^{\ell-1} \sum_{t \in \mathbb{F}_q} S^{i+j}((t-1)(t^2+\lambda)) \\ &\quad + \sum_{i, j=1, i \neq j, i+j \neq \ell}^{\ell-1} \sum_{t \in \mathbb{F}_q} S^{i+j}((t-1)(t^2+\lambda)). \end{aligned}$$

Then Lemma 1.3.7 yields

$$\begin{aligned} a_q(V_{\ell,\lambda})^2 &= \sum_{i=1}^{\ell-1} S^i(\lambda^2)g\left(S^i, S^i; -\frac{1}{\lambda}\right)^2 + 2(q-1) \cdot \lfloor \frac{\ell-1}{2} \rfloor \\ &\quad + \sum_{i,j=1, i \neq j, i+j \neq \ell}^{\ell-1} \sum_{t \in \mathbb{F}_q} S^{i+j}((t-1)(t^2+\lambda)). \end{aligned} \quad (4.3.8)$$

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

$$\begin{aligned} g\left(S^i, S^i; -\frac{1}{\lambda}\right)^2 &= q^2 \cdot \frac{S^i(-4\lambda)J(S^{-3i}, S^i)}{J(S^{-i}, S^{-i})} \cdot {}_3F_2\left(\begin{matrix} S^{-3i}, & S^{-i}, & S^{-2i}\phi \\ & S^{-4i}, & S^{-2i} \end{matrix} \middle| \frac{1+\lambda}{\lambda}\right) \\ &\quad + q \cdot \frac{\phi(-\lambda)S^i(-\frac{4(1+\lambda)^2}{\lambda})J(S^{-3i}, S^i)}{J(S^{-i}, S^{-i})}. \end{aligned} \quad (4.3.9)$$

Now we find the value of

$$\sum_{i,j=1, i \neq j, i+j \neq \ell}^{\ell-1} \sum_{t \in \mathbb{F}_q} S^{i+j}((t-1)(t^2+\lambda)).$$

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  $\ell$

$$\#P(i_k) = \begin{cases} \ell - 2, & \text{if } k \text{ is odd;} \\ \ell - 4, & \text{if } k \text{ is even.} \end{cases}$$

Therefore,

$$\begin{aligned} &\sum_{i,j=1, i \neq j, i+j \neq \ell}^{\ell-1} \sum_{t \in \mathbb{F}_q} S^{i+j}((t-1)(t^2+\lambda)) \\ &= \begin{cases} (\ell-3) \sum_{i=1}^{\ell-1} \sum_{t \in \mathbb{F}_q} S^i((t-1)(t^2+\lambda)), & \text{if } \ell \text{ is odd;} \\ (\ell-2) \sum_{i=1}^{\ell-1} \sum_{t \in \mathbb{F}_q} S^i((t-1)(t^2+\lambda)) - 2 \sum_{i=1}^{\frac{\ell}{2}-1} \sum_{t \in \mathbb{F}_q} S^{2i}((t-1)(t^2+\lambda)), & \text{if } \ell \text{ is even.} \end{cases} \end{aligned}$$

From (4.3.7), (4.2.3) and Theorem 4.2.1, we deduce that

$$\begin{aligned}
& \sum_{i,j=1, i \neq j, i+j \neq \ell}^{\ell-1} \sum_{t \in \mathbb{F}_q} S^{i+j} ((t-1)(t^2 + \lambda)) \\
&= \begin{cases} -(\ell-3)a_q(V_{\ell,\lambda}), & \text{if } \ell \text{ is odd;} \\ -(\ell-2)a_q(V_{\ell,\lambda}) \\ -2q \sum_{i=1}^{\frac{\ell}{2}-1} \frac{J(\phi, S^{2i})}{J(S^{-i}, S^{3i}\phi)} \cdot {}_2F_1 \left( \begin{matrix} S^{-3i}\phi, & S^{-3i} \\ & S^{-4i} \end{matrix} \middle| 1 + \lambda \right), & \text{if } \ell \text{ is even.} \end{cases}
\end{aligned} \tag{4.3.10}$$

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

$$a_q(V_{2,\lambda})^2 = q^2 \phi(-\lambda) \cdot {}_3F_2 \left( \begin{matrix} \phi, & \phi, & \phi \\ \varepsilon, & \varepsilon & \end{matrix} \middle| \frac{1+\lambda}{\lambda} \right) + q, \tag{4.3.11}$$

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

$$-a_q(V_{\ell,\lambda}) = q \cdot \sum_{i=1}^{\frac{\ell-1}{2}} \frac{J(\phi, S^{-i})}{J(\sqrt{S^i}, \sqrt{S^{-3i}\phi})} \cdot {}_2F_1 \left( \begin{matrix} \sqrt{S^{3i}\phi}, & \sqrt{S^{3i}} \\ & S^{2i} \end{matrix} \middle| 1 + \lambda \right) \tag{4.3.12}$$

and for  $\ell = 3$ ,

$$-a_q(V_{\ell,\lambda}) = 2 + q \cdot \sum_{i=1}^2 {}_2F_1 \left( \begin{matrix} \phi, & \varepsilon \\ & S^i \end{matrix} \mid 1 + \lambda \right), \quad (4.3.13)$$

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

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

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

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

As  $\frac{q-1}{\ell}$  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

$$g(S^i, S^i; -\frac{1}{\lambda}) = \frac{qS^i(-\frac{1}{\lambda})J(\phi, S^i)}{J(\sqrt{S^{-i}}, \sqrt{S^{3i}}\phi)} \cdot {}_2F_1 \left( \begin{matrix} \sqrt{S^{-3i}}\phi, & \sqrt{S^{-3i}} \\ & S^{-2i} \end{matrix} \mid 1 + \lambda \right). \quad (4.3.17)$$

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

$$\begin{aligned} & \#\{(x, y) \in \mathbb{F}_q^2 : y^\ell = (x-1)(x^2 + \lambda)\} \\ &= q + \sum_{i=1}^{\ell-1} S^i(-\lambda)g \left( S^i, S^i; -\frac{1}{\lambda} \right) \\ &= q + q \cdot \sum_{i=1}^{\ell-1} \frac{J(\phi, S^i)}{J(\sqrt{S^{-i}}, \sqrt{S^{3i}}\phi)} \cdot {}_2F_1 \left( \begin{matrix} \sqrt{S^{-3i}}\phi, & \sqrt{S^{-3i}} \\ & S^{-2i} \end{matrix} \mid 1 + \lambda \right). \end{aligned}$$

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

$$\begin{aligned} g(S^i, S^i; -\frac{1}{\lambda}) &= qS^i(-\frac{8}{\lambda})F^*(\varepsilon, S^i; 1 + \lambda) \\ &= qS^i(-\frac{1}{\lambda}){}_2F_1\left(\begin{matrix} \phi, & \varepsilon \\ & S^i \end{matrix} \middle| 1 + \lambda\right) \end{aligned} \quad (4.3.18)$$

Now combining (4.3.18) with (4.3.14) and (4.3.15), we deduce that

$$\begin{aligned} \#\{(x, y) \in \mathbb{F}_q^2 : y^\ell = (x-1)(x^2 + \lambda)\} &= q + \sum_{i=1}^{\ell-1} S^i(-\lambda)g\left(S^i, S^i; -\frac{1}{\lambda}\right) \\ &= q + q \cdot \sum_{i=1}^2 {}_2F_1\left(\begin{matrix} \phi, & \varepsilon \\ & S^i \end{matrix} \middle| 1 + \lambda\right) \end{aligned}$$

which yields the result because of (4.3.4).  $\square$

**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

$$p \cdot \sum_{i=1}^2 {}_2F_1\left(\begin{matrix} \phi, & \varepsilon \\ & \chi_3^i \end{matrix} \middle| \frac{1}{2}\right) = \phi(2)(-1)^{x+y} \left(\frac{x}{3}\right) \cdot 2x - 2,$$

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

$$\begin{aligned} a_p(V_{3, -\frac{1}{2}}) &= \phi(2)a_p(E') \\ &= \phi(2)(-1)^{x+y-1} \left(\frac{x}{3}\right) \cdot 2x. \end{aligned} \quad (4.3.19)$$

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

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*

$${}_3F_2 \left( \begin{matrix} \phi, & \phi, & \phi \\ & \varepsilon, & \varepsilon \end{matrix} \middle| \frac{1+\lambda}{\lambda} \right) = \phi(\lambda) {}_2F_1 \left( \begin{matrix} \overline{\chi}_4, & \chi_4 \\ & \varepsilon \end{matrix} \middle| 1+\lambda \right)^2 - \frac{\phi(\lambda)}{q},$$

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

$$a_q(V_{2,\lambda})^2 = q^2 \cdot \frac{J(\phi, \phi)^2}{J(\chi_4, \overline{\chi}_4)^2} \cdot {}_2F_1 \left( \begin{matrix} \overline{\chi}_4, & \chi_4 \\ & \varepsilon \end{matrix} \middle| 1+\lambda \right)^2.$$

By (1.3.2), we have  $J(\phi, \phi) = J(\chi_4, \overline{\chi}_4)$ . Hence comparing with (4.3.11), we complete the proof.  $\square$

**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  $\text{ord}_p\left(\frac{4(4-\alpha^2)}{\alpha^4}\right) = 0$ , then*

$${}_2F_1 \left( \begin{matrix} \phi, & \phi \\ & \varepsilon \end{matrix} \middle| \frac{\alpha-2}{\alpha+2} \right)^2 = \phi(4-\alpha^2) {}_3F_2 \left( \begin{matrix} \phi, & \phi, & \phi \\ & \varepsilon, & \varepsilon \end{matrix} \middle| \frac{4}{4-\alpha^2} \right) + \frac{1}{q}.$$

*Proof.* Replacing  $\lambda$  by  $\frac{4-\alpha^2}{\alpha^2}$  in Corollary 4.3.4, we have

$${}_2F_1 \left( \begin{matrix} \overline{\chi}_4, \chi_4 \\ \varepsilon \end{matrix} \middle| \frac{4}{\alpha^2} \right)^2 = \phi(4-\alpha^2) {}_3F_2 \left( \begin{matrix} \phi, \phi, \phi \\ \varepsilon, \varepsilon \end{matrix} \middle| \frac{4}{4-\alpha^2} \right) + \frac{1}{q}.$$

Again, from Corollary 2.3.3, we obtain

$${}_2F_1 \left( \begin{matrix} \overline{\chi}_4, \chi_4 \\ \varepsilon \end{matrix} \middle| \frac{4}{\alpha^2} \right)^2 = {}_2F_1 \left( \begin{matrix} \phi, \phi \\ \varepsilon \end{matrix} \middle| \frac{\alpha-2}{\alpha+2} \right)^2.$$

Hence the proof follows.  $\square$

#### 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*

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

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  $(x, y) \rightarrow (\frac{x}{9} + \frac{1}{3}, y)$ , 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,

$$\begin{aligned} & \#\{(x, y) \in \mathbb{F}_q^2 : y^\ell = (x-1)(x^2 + \frac{1}{3})\} \\ &= \#\{(x, y) \in \mathbb{F}_q^2 : y^\ell = -\frac{8}{27}(1+x^3)\} \\ &= \sum_{x \in \mathbb{F}_q, 1+x^3 \neq 0} \#\{y \in \mathbb{F}_q : y^\ell = -\frac{8}{27}(1+x^3)\} + \#\{x \in \mathbb{F}_q : 1+x^3 = 0\} \end{aligned}$$

Applying Lemma 1.3.6, we obtain

$$\#\{(x, y) \in \mathbb{F}_q^2 : y^\ell = (x-1)(x^2 + \frac{1}{3})\} = q + \sum_{i=1}^{\ell-1} \sum_{x \in \mathbb{F}_q} S^i(-\frac{8}{27}) S^i(1+x^3).$$

Now recall that the binomial theorem (see [18]) for a character  $A$  on  $\mathbb{F}_q$  is given by

$$A(1+x) = \delta(x) + \frac{q}{q-1} \sum_x \binom{A}{\chi} \chi(x),$$

where  $\delta(x) = 1$  (resp. 0) if  $x = 0$  (resp.  $x \neq 0$ ). Hence

$$\begin{aligned} & \#\{(x, y) \in \mathbb{F}_q^2 : y^\ell = (x-1)(x^2 + \frac{1}{3})\} \\ &= q + \sum_{i=1}^{\ell-1} \sum_{x \in \mathbb{F}_q} S^i(-\frac{8}{27}) \left[ \delta(x^3) + \frac{q}{q-1} \sum_x \binom{S^i}{\chi} \chi(x^3) \right] \\ &= q + \sum_{i=1}^{\ell-1} S^i(-\frac{8}{27}) + \frac{q}{q-1} \sum_{i=0}^{\ell-1} S^i(-\frac{8}{27}) \sum_x \binom{S^i}{\chi} \sum_{x \in \mathbb{F}_q} \chi^3(x). \quad (4.4.1) \end{aligned}$$

By Lemma 1.3.7,  $\sum_{x \in \mathbb{F}_q} \chi^3(x)$  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

$$\begin{aligned} & \#\{(x, y) \in \mathbb{F}_q^2 : y^\ell = (x-1)(x^2 + \frac{1}{3})\} \\ &= \begin{cases} q, & \text{if } q \equiv 2 \pmod{3}; \\ q + q \cdot \sum_{i=1}^{\ell-1} S^i(\frac{27}{8}) \left[ \binom{\chi_3}{S^i} + \binom{\chi_3^2}{S^i} \right], & \text{if } q \equiv 1 \pmod{3}, \end{cases} \end{aligned}$$

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*

$$-\frac{\phi(-2)}{q} \cdot a_q(V_{2, \frac{1}{3}}) = 2\operatorname{Re} \left( \binom{\chi_3}{\phi} \right)$$

and

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

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

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

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  $\overline{\binom{\chi_3}{\phi}} = \binom{\chi_3^2}{\phi}$ .

Again the second part follows from the fact that if  $\chi\bar{\psi}$  is nontrivial, then

$$\binom{\chi}{\psi} = \frac{\psi(-1)}{q} J(\chi, \bar{\psi}) = \frac{\psi(-1)}{q} \frac{G(\chi)G(\bar{\psi})}{G(\chi\bar{\psi})},$$

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

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  $d = \operatorname{lcm}(3, \ell)$ . If  $q \equiv 1 \pmod{d}$ , then*

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

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.  $\square$

# Chapter 5

## On The Polynomial $x^d + ax + b$ and Gaussian Hypergeometric Series

### 5.1 Introduction

In the previous chapters, we have discussed about connections between number of points on algebraic curves over  $\mathbb{F}_q$  and Gaussian hypergeometric functions. In all those expressions only  ${}_2F_1$  and  ${}_3F_2$  Gaussian hypergeometric functions are involved containing characters of different orders as parameters.

The problem of finding special values of  ${}_{n+1}F_n$  Gaussian hypergeometric series for  $n > 2$  was discussed by many mathematicians. For  $n > 2$ , the non-trivial values of  ${}_{n+1}F_n$  Gaussian hypergeometric series have been difficult to obtain. For example, Ono and Ahlgren-Ono mentioned this problem in [35] and [1], respectively. In [1], Ahlgren and Ono deduced the value of  ${}_4F_3 \left( \begin{matrix} \phi, & \phi, & \phi, & \phi \\ \varepsilon, & \varepsilon, & \varepsilon & | 1 \end{matrix} \right)$  in terms of representations of  $4p$  as a sum of four squares. The deduction of the value relies on the fact that the Calabi-Yau threefold is modular. Except this, there is not much known results in literature where expressions of different mathematical objects can be obtained in terms of  ${}_{n+1}F_n$  Gaussian hypergeometric series for  $n > 2$ .

In this chapter, we consider this problem and explicitly find the number of solutions of a polynomial equation  $P_d(x) = 0$  of degree  $d$  in  $\mathbb{F}_q$  as special values of  ${}_dF_{d-1}$  and  ${}_{d-1}F_{d-2}$  Gaussian hypergeometric series with characters of orders  $d$  and  $d - 1$

---

<sup>4</sup>The contents of this chapter have appeared in *Int. J. Number Theory* (2013).

as parameters. Thus these expressions partially solve a problem posed by Ken Ono [35, p. 204] on special values of  ${}_{n+1}F_n$  Gaussian hypergeometric series for  $n > 2$ .

## 5.2 Main results

First of all we look into two special cases of Hasse-Davenport relation. Then we state our main results of this section in detail and subsequently prove them using the following two special cases.

**Lemma 5.2.1.** *Let  $d$  be a positive integer,  $l \in \mathbb{Z}$ ,  $q = p^e \equiv 1 \pmod{d}$ , and  $t \in \{1, -1\}$ .*

1. *If  $d > 1$  is odd, then*

$$G_l G_{l+t\frac{q-1}{d}} G_{l+t\frac{2(q-1)}{d}} \cdots G_{l+t\frac{(d-1)(q-1)}{d}} = q^{\frac{d-1}{2}} T^{\frac{(d-1)(d+1)(q-1)}{8d}} (-1) T^{-l} (d^d) G_{ld}. \quad (5.2.1)$$

2. *If  $d$  is even, then*

$$G_l G_{l+t\frac{q-1}{d}} G_{l+t\frac{2(q-1)}{d}} \cdots G_{l+t\frac{(d-1)(q-1)}{d}} = q^{\frac{d-2}{2}} G_{\frac{q-1}{2}} T^{\frac{(d-2)(q-1)}{8}} (-1) T^{-l} (d^d) G_{ld}. \quad (5.2.2)$$

*Proof.* Let  $d > 1$  be an odd integer and consider  $m = d$  in Lemma 1.3.17. Since  $q \equiv 1 \pmod{d}$ , there are  $d$  multiplicative characters of order dividing  $d$ , namely,  $\varepsilon, T^{\frac{q-1}{d}}, T^{\frac{2(q-1)}{d}}, \dots, T^{\frac{(d-1)(q-1)}{d}}$ . Applying Hasse-Davenport relation for these characters and for any arbitrary multiplicative character  $T^l$  of  $\mathbb{F}_q$ , we have

$$\begin{aligned} & G(T^l) G(T^{l+\frac{q-1}{d}}) \cdots G(T^{l+\frac{(d-1)(q-1)}{d}}) \\ &= -G(T^{ld}) T^l (d^{-d}) G(\varepsilon) G(T^{\frac{q-1}{d}}) \cdots G(T^{\frac{(d-1)(q-1)}{d}}) \\ &= -G_{ld} T^{-l} (d^d) G_0 \left\{ G_{\frac{q-1}{d}} G_{\frac{(d-1)(q-1)}{d}} \right\} \cdots \left\{ G_{\frac{(d-1)(q-1)}{2d}} G_{\frac{(d+1)(q-1)}{2d}} \right\}. \end{aligned}$$

Using Lemma 1.3.10, and the fact  $G_0 = G(\varepsilon) = -1$ , we obtain

$$\begin{aligned} & G_l G_{l+\frac{q-1}{d}} \cdots G_{l+\frac{(d-1)(q-1)}{d}} \\ &= G_{ld} T^{-l}(d^d) \left\{ q T^{\frac{q-1}{d}}(-1) \right\} \cdots \left\{ q T^{\frac{(d-1)(q-1)}{2d}}(-1) \right\} \\ &= q^{\frac{d-1}{2}} T^{\frac{(d-1)(d+1)(q-1)}{8d}}(-1) T^{-l}(d^d) G_{ld} \end{aligned}$$

as required. To get the other equality, we use Hasse-Davenport relation for the  $d$  characters  $\varepsilon, T^{-\frac{q-1}{d}}, \dots, T^{-\frac{(d-1)(q-1)}{d}}$ . Thus we complete the proof of (5.2.1).

For even values of  $d \geq 2$ , the proof of (5.2.2) follows similarly to that of (5.2.1) by virtue of Hasse-Davenport relation.  $\square$

We are now going to state and prove our main results. Throughout the chapter, for  $d \geq 2$ , we consider the polynomial

$$P_d(x) := x^d + ax + b$$

over  $\mathbb{F}_q$ , where  $a, b \neq 0$ . For even and odd values of  $d$ , we find separate expressions for the number of points on  $P_d$  over  $\mathbb{F}_q$  in terms of  ${}_{d-1}F_{d-2}$  and  ${}_dF_{d-1}$  Gaussian hypergeometric functions, respectively. The method of the proofs follow similarly to that given in [14] and [27].

### 5.2.1 Number of zeros of $x^d + ax + b$ for even $d$

**Theorem 5.2.2.** *Let  $d \geq 2$  be an even integer and  $q \equiv 1 \pmod{d(d-1)}$ . If  $N_d$  is the number of distinct solutions in  $\mathbb{F}_q$  of the polynomial equation  $P_d(x) = 0$ , then*

$$N_d = 1 + q^{\frac{d-2}{2}} \times {}_{d-1}F_{d-2} \left( \begin{matrix} \phi, \chi, \dots, \chi^{\frac{d-2}{2}}, \chi^{\frac{d+2}{2}}, \dots, \chi^{d-1} \\ \psi, \dots, \psi^{\frac{d-2}{2}}, \psi^{\frac{d}{2}}, \dots, \psi^{d-2} \end{matrix} \middle| \frac{d}{a} \left( \frac{bd}{a(d-1)} \right)^{d-1} \right),$$

where  $\psi$  and  $\chi$  are characters of order  $d-1$  and  $d$ , respectively.

*Proof.* We first recall that the polynomial  $P_d(x)$  defined over  $\mathbb{F}_q$  is given by

$$P_d(x) = x^d + ax + b,$$

where  $a, b \neq 0$ . We also have

$$N_d = \#\{\alpha \in \mathbb{F}_q : P_d(\alpha) = 0\},$$

the number of distinct zeros of the polynomial  $P_d(x)$  in  $\mathbb{F}_q$ . Using (1.3.1) for the polynomial  $P_d(x)$ , we have

$$\sum_{z \in \mathbb{F}_q} \theta(zP_d(x)) = \begin{cases} q & \text{if } P_d(x) = 0; \\ 0 & \text{if } P_d(x) \neq 0, \end{cases} \quad (5.2.3)$$

and hence

$$\begin{aligned} q \cdot N_d &= \sum_{x, z \in \mathbb{F}_q} \theta(zP_d(x)) \\ &= q + \sum_{z \in \mathbb{F}_q^\times} \theta(zb) + \sum_{x, z \in \mathbb{F}_q^\times} \theta(zx^d)\theta(zax)\theta(zb) \\ &:= q + A + B. \end{aligned} \quad (5.2.4)$$

Now using Lemma 1.3.11 and then applying Lemma 1.3.7 repeatedly for each term of (5.2.4), we deduce that

$$A = \frac{1}{q-1} \sum_{z \in \mathbb{F}_q^\times} \sum_{l=0}^{q-2} G_{-l} T^l(zb) = \frac{1}{q-1} \sum_{l=0}^{q-2} G_{-l} T^l(b) \sum_{z \in \mathbb{F}_q^\times} T^l(z) = -1. \quad (5.2.5)$$

The second equality follows from the facts that the innermost sum is nonzero only if  $l = 0$ , at which it is  $q - 1$ , and  $G_0 = -1$ . Similarly,

$$B = \frac{1}{(q-1)^3} \sum_{l, m, n=0}^{q-2} G_{-l} G_{-m} G_{-n} T^m(a) T^m(b) \sum_{z \in \mathbb{F}_q^\times} T^{l+m+n}(z) \sum_{x \in \mathbb{F}_q^\times} T^{ld+m}(z).$$

This term is zero unless  $m = -ld$  and  $n = l(d-1)$ . Plugging these values, we have

$$B = \frac{1}{q-1} \sum_{l=0}^{q-2} G_{-l} G_{ld} G_{-l(d-1)} T^l \left( \frac{b^{d-1}}{a^d} \right). \quad (5.2.6)$$

Here  $d \geq 2$  is even. Using the Hasse-Davenport relations for  $G_{ld}$  and  $G_{-l(d-1)}$  as given in (5.2.2) and (5.2.1), we deduce that

$$G_{ld} = \frac{G_l G_{l+\frac{q-1}{d}} G_{l+\frac{2(q-1)}{d}} \cdots G_{l+\frac{(d-1)(q-1)}{d}}}{q^{\frac{d-2}{2}} G_{\frac{q-1}{2}} T^{\frac{(d-2)(q-1)}{8}}(-1)} T^l(d^d) \quad (5.2.7)$$

and

$$G_{-l(d-1)} = \frac{G_{-l} G_{-l-\frac{q-1}{d-1}} G_{-l-\frac{2(q-1)}{d-1}} \cdots G_{-l-\frac{(d-2)(q-1)}{d-1}}}{q^{\frac{d-2}{2}} T^{\frac{d(d-2)(q-1)}{8(d-1)}}(-1) T^l((d-1)^{d-1})}. \quad (5.2.8)$$

Using (5.2.7) and (5.2.8) in (5.2.6), we obtain

$$\begin{aligned} B &= \frac{T^{\frac{(d-2)(q-1)}{8(d-1)}}(-1)}{(q-1)q^{d-2}G_{\frac{q-1}{2}}} \sum_{l=0}^{q-2} \{G_l G_{-l}\} \left\{ G_{l+\frac{d}{2}\frac{q-1}{d}} G_{-l} \right\} \left\{ G_{l+\frac{(q-1)}{d}} G_{-l-\frac{q-1}{d-1}} \right\} \cdots \\ &\quad \times \left\{ G_{l+\frac{(d-2)(q-1)}{2d}} G_{-l-\frac{(d-2)(q-1)}{2(d-1)}} \right\} \left\{ G_{l+\frac{(d+2)(q-1)}{2d}} G_{-l-\frac{d(q-1)}{2(d-1)}} \right\} \cdots \\ &\quad \times \left\{ G_{l+\frac{(d-1)(q-1)}{d}} G_{-l-\frac{(d-2)(q-1)}{d-1}} \right\} T^l(\beta), \end{aligned} \quad (5.2.9)$$

where

$$\beta = \frac{d}{a} \left( \frac{bd}{a(d-1)} \right)^{d-1}.$$

To eliminate  $G_l G_{-l}$ , we use the facts that if  $l \neq 0$ , then  $G_l G_{-l} = qT^l(-1)$ ; and if  $l = 0$ , then  $G_l G_{-l} = 1 = qT^l(-1) - (q-1)$  in appropriate identities of (5.2.9) and deduce that

$$\begin{aligned} B &= \frac{T^{\frac{(d-2)(q-1)}{8(d-1)}}(-1)}{(q-1)q^{d-3}G_{\frac{q-1}{2}}} \sum_{l=0}^{q-2} \left\{ G_{l+\frac{q-1}{2}} G_{-l} \right\} \left\{ G_{l+\frac{(q-1)}{d}} G_{-l-\frac{q-1}{d-1}} \right\} \cdots \\ &\quad \times \left\{ G_{l+\frac{(d-2)(q-1)}{2d}} G_{-l-\frac{(d-2)(q-1)}{2(d-1)}} \right\} \left\{ G_{l+\frac{(d+2)(q-1)}{2d}} G_{-l-\frac{d(q-1)}{2(d-1)}} \right\} \cdots \\ &\quad \times \left\{ G_{l+\frac{(d-1)(q-1)}{d}} G_{-l-\frac{(d-2)(q-1)}{d-1}} \right\} T^l(-\beta) + \frac{T^{\frac{(d-2)(q-1)}{8(d-1)}}(-1)}{q^{d-2}} \left\{ G_{\frac{(q-1)}{d}} G_{-\frac{q-1}{d-1}} \right\} \cdots \\ &\quad \times \left\{ G_{\frac{(d-2)(q-1)}{2d}} G_{-\frac{(d-2)(q-1)}{2(d-1)}} \right\} \left\{ G_{\frac{(d+2)(q-1)}{2d}} G_{-\frac{d(q-1)}{2(d-1)}} \right\} \cdots \left\{ G_{\frac{(d-1)(q-1)}{d}} G_{-\frac{(d-2)(q-1)}{d-1}} \right\}. \end{aligned}$$

Now, we rearrange the Gauss sums of the second term to get

$$\begin{aligned}
B &= \frac{T^{\frac{(d-2)(q-1)}{8(d-1)}} (-1)}{(q-1)q^{d-3}G_{\frac{q-1}{2}}} \sum_{l=0}^{q-2} \left\{ G_{l+\frac{q-1}{2}} G_{-l} \right\} \left\{ G_{l+\frac{(q-1)}{d}} G_{-l-\frac{q-1}{d-1}} \right\} \cdots \\
&\quad \times \left\{ G_{l+\frac{(d-2)(q-1)}{2d}} G_{-l-\frac{(d-2)(q-1)}{2(d-1)}} \right\} \left\{ G_{l+\frac{(d+2)(q-1)}{2d}} G_{-l-\frac{d(q-1)}{2(d-1)}} \right\} \cdots \\
&\quad \times \left\{ G_{l+\frac{(d-1)(q-1)}{d}} G_{-l-\frac{(d-2)(q-1)}{d-1}} \right\} T^l(-\beta) + \frac{T^{\frac{(d-2)(q-1)}{8(d-1)}} (-1)}{q^{d-2}} \left\{ G_{\frac{(q-1)}{d}} G_{\frac{(d-1)(q-1)}{d}} \right\} \\
&\quad \times \left\{ G_{-\frac{q-1}{d-1}} G_{-\frac{(d-2)(q-1)}{d-1}} \right\} \cdots \left\{ G_{\frac{(d-2)(q-1)}{2d}} G_{\frac{(d+2)(q-1)}{2d}} \right\} \left\{ G_{-\frac{(d-2)(q-1)}{2(d-1)}} G_{-\frac{d(q-1)}{2(d-1)}} \right\}.
\end{aligned}$$

But,  $G_{\frac{(d-1)(q-1)}{d}} = G_{-\frac{(q-1)}{d}}$ ,  $G_{-\frac{(d-2)(q-1)}{d-1}} = G_{\frac{q-1}{d-1}}$ , and so on. Using Lemma 1.3.12 in the first term and Lemma 1.3.10 in the second term, we have

$$\begin{aligned}
B &= \frac{q^2 T^{\frac{(d-2)(q-1)}{8(d-1)}} (-1)}{(q-1)G_{\frac{q-1}{2}}} \sum_{l=0}^{q-2} \begin{pmatrix} T^{l+\frac{q-1}{2}} \\ T^l \end{pmatrix} G_{\frac{q-1}{2}} \begin{pmatrix} T^{l+\frac{(q-1)}{d}} \\ T^{l+\frac{q-1}{d-1}} \end{pmatrix} G_{-\frac{q-1}{d-1}} \cdots \begin{pmatrix} T^{l+\frac{(d-2)(q-1)}{2d}} \\ T^{l+\frac{(d-2)(q-1)}{2(d-1)}} \end{pmatrix} \times \\
&\quad G_{-\frac{(d-2)(q-1)}{2d(d-1)}} \begin{pmatrix} T^{l+\frac{(d+2)(q-1)}{2d}} \\ T^{l+\frac{d(q-1)}{2(d-1)}} \end{pmatrix} G_{\frac{(d-2)(q-1)}{2d(d-1)}} \begin{pmatrix} T^{l+\frac{(d-1)(q-1)}{d}} \\ T^{l+\frac{(d-2)(q-1)}{d-1}} \end{pmatrix} G_{\frac{q-1}{d(d-1)}} T^l(\beta) + \frac{T^{\frac{(d-2)(q-1)}{8(d-1)}} (-1)}{q^{d-2}} \\
&\quad \times \left\{ qT^{\frac{(q-1)}{d}} (-1) \right\} \left\{ qT^{\frac{(q-1)}{d-1}} (-1) \right\} \cdots \left\{ qT^{\frac{(d-2)(q-1)}{2d}} (-1) \right\} \left\{ qT^{\frac{(d-2)(q-1)}{2(d-1)}} (-1) \right\}.
\end{aligned}$$

Finally, we use Lemma 1.3.10 again, and simplify to get

$$B = 1 + q^{\frac{d}{2}d-1} F_{d-2} \left( \begin{array}{c} \phi, \chi, \dots, \chi^{\frac{d-2}{2}}, \chi^{\frac{d+2}{2}}, \dots, \chi^{d-1} \\ \psi, \dots, \psi^{\frac{d-2}{2}}, \psi^{\frac{d}{2}}, \dots, \psi^{d-2} \mid \beta \end{array} \right).$$

Substituting the values of  $A$  and  $B$  in (5.2.4), we have

$$q \cdot N_d = q + q^{\frac{d}{2}d-1} F_{d-2} \left( \begin{array}{c} \phi, \chi, \dots, \chi^{\frac{d-2}{2}}, \chi^{\frac{d+2}{2}}, \dots, \chi^{d-1} \\ \psi, \dots, \psi^{\frac{d-2}{2}}, \psi^{\frac{d}{2}}, \dots, \psi^{d-2} \mid \beta \end{array} \right).$$

Canceling  $q$  from both sides, we complete the proof of the theorem.  $\square$



### 5.2.2 Number of zeros of $x^d + ax + b$ for odd $d$

**Theorem 5.2.3.** *Let  $d > 2$  be an odd integer and  $q \equiv 1 \pmod{d(d-1)}$ . If  $N_d$  is the number of distinct solutions in  $\mathbb{F}_q$  of the polynomial equation  $P_d(x) = 0$ , then*

$$N_d = 1 - \frac{\phi(-ad)}{q} + q^{\frac{d-1}{2}} \phi(-1) \times \\ {}_dF_{d-1} \left( \begin{matrix} \phi, \chi, \dots, \chi^{\frac{d-1}{2}}, \chi^{\frac{d+1}{2}}, \dots, \chi^{d-1} \\ \psi, \dots, \psi^{\frac{d-1}{2}}, \psi^{\frac{d-1}{2}}, \dots, \psi^{d-2} \end{matrix} \mid -\frac{d}{a} \left( \frac{bd}{a(d-1)} \right)^{d-1} \right),$$

where  $\psi$  and  $\chi$  are characters of order  $d-1$  and  $d$ , respectively.

*Proof.* We follow the same procedure as followed in the proof of Theorem 5.2.2. We have

$$P_d(x) = x^d + ax + b$$

and

$$N_d = \{\alpha \in \mathbb{F}_q : P_d(\alpha) = 0\}.$$

From the proof of Theorem 5.2.2, we know that

$$q \cdot N_d = q - 1 + \underbrace{\frac{1}{q-1} \sum_{l=0}^{q-2} G_{-l} G_{ld} G_{-l(d-1)} T^l \left( \frac{b^{d-1}}{a^d} \right)}_B. \quad (5.2.10)$$

Here  $d \geq 3$  is odd. We evaluate the labeled term  $B$  using the Hasse-Davenport relation for  $G_{ld}$  and  $G_{-l(d-1)}$  from (5.2.1) and (5.2.2). We have

$$G_{ld} = \frac{G_l G_{l+\frac{q-1}{d}} G_{l+\frac{2(q-1)}{d}} \cdots G_{l+\frac{(d-1)(q-1)}{d}}}{q^{\frac{d-1}{2}} T^{\frac{(d-1)(d+1)(q-1)}{8d}} (-1)} T^l (d^d)$$

and

$$G_{-l(d-1)} = \frac{G_{-l} G_{-l-\frac{q-1}{d-1}} G_{-l-\frac{2(q-1)}{d-1}} \cdots G_{-l-\frac{(d-2)(q-1)}{d-1}}}{q^{\frac{d-3}{2}} G_{\frac{q-1}{2}} T^{\frac{(d-3)(q-1)}{8}} (-1)} T^{-l} ((d-1)^{d-1}).$$

Plugging these in the labeled term of (5.2.10), we deduce that

$$B = \frac{T^{\frac{(3d-1)(q-1)}{8d}}(-1)}{(q-1)q^{d-2}G_{\frac{q-1}{2}}} \sum_{l=0}^{q-2} \{G_l G_{-l}\} \left\{ G_{l+\frac{q-1}{d}} \cdots G_{l+\frac{(d-1)(q-1)}{d}} \right\} \\ \times \left\{ G_{-l} G_{-l-\frac{q-1}{d-1}} \cdots G_{-l-\frac{(d-2)(q-1)}{d-1}} \right\} T^l(\beta),$$

where

$$\beta = \frac{d}{a} \left( \frac{bd}{a(d-1)} \right)^{d-1}.$$

The facts  $G_l G_{-l} = qT^l(-1)$  if  $l \neq 0$ , and  $G_l G_{-l} = qT^l(-1) - (q-1)$  if  $l = 0$  together yield that

$$B = \frac{T^{\frac{(3d-1)(q-1)}{8d}}(-1)}{(q-1)q^{d-3}G_{\frac{q-1}{2}}} \sum_{l=0}^{q-2} \left\{ G_{l+\frac{q-1}{d}} \cdots G_{l+\frac{(d-1)(q-1)}{d}} \right\} \left\{ G_{-l} G_{-l-\frac{q-1}{d-1}} \cdots G_{-l-\frac{(d-2)(q-1)}{d-1}} \right\} \\ \times T^l(-\beta) + \frac{T^{\frac{(3d-1)(q-1)}{8d}}(-1)}{q^{d-2}} \left\{ G_{\frac{q-1}{d}} G_{\frac{(d-1)(q-1)}{d}} \right\} \left\{ G_{-\frac{q-1}{d-1}} G_{-\frac{(d-2)(q-1)}{d-1}} \right\} \cdots \\ \times \left\{ G_{\frac{(d-1)(q-1)}{2d}} G_{\frac{(d+1)(q-1)}{2d}} \right\} \left\{ G_{\frac{(d-3)(q-1)}{2(d-1)}} G_{-\frac{(d+1)(q-1)}{2(d-1)}} \right\}. \quad (5.2.11)$$

Again, using

$$G_{l+\frac{q-1}{2}} G_{-l-\frac{q-1}{2}} = \begin{cases} qT^{l+\frac{q-1}{2}}(-1), & \text{if } l \neq \frac{q-1}{2}; \\ qT^{l+\frac{q-1}{2}}(-1) - (q-1), & \text{if } l = \frac{q-1}{2} \end{cases}$$

for appropriate values of  $l$ , we have

$$\sum_{l=0}^{q-2} \left\{ G_{l+\frac{q-1}{d}} \cdots G_{l+\frac{(d-1)(q-1)}{d}} \right\} \left\{ G_{-l} G_{-l-\frac{q-1}{d-1}} \cdots G_{-l-\frac{(d-2)(q-1)}{d-1}} \right\} T^l(-\beta) \\ = \frac{1}{qT^{\frac{q-1}{2}}} \sum_{l=0}^{q-2} \left\{ G_{l+\frac{q-1}{2}} G_{-l} \right\} \left\{ G_{l+\frac{(q-1)}{d}} G_{-l-\frac{q-1}{d-1}} \right\} \cdots \left\{ G_{l+\frac{(d-1)(q-1)}{2d}} G_{-l-\frac{(d-1)(q-1)}{2(d-1)}} \right\} \\ \times \left\{ G_{l+\frac{(d+1)(q-1)}{2d}} G_{-l-\frac{(d-1)(q-1)}{2(d-1)}} \right\} \cdots \left\{ G_{l+\frac{(d-1)(q-1)}{d}} G_{-l-\frac{(d-2)(q-1)}{d-1}} \right\} T^l(\beta) \\ - \frac{(q-1)G_{\frac{q-1}{2}}}{qT^{\frac{q-1}{2}}(-ad)} \left\{ G_{\frac{(d+2)(q-1)}{2d}} G_{\frac{(3d-2)(q-1)}{2d}} \right\} \left\{ G_{-\frac{(d+1)(q-1)}{2(d-1)}} G_{-\frac{(3d-5)(q-1)}{2(d-1)}} \right\} \cdots \\ \times \left\{ G_{\frac{(2d-1)(q-1)}{2d}} G_{\frac{(2d+1)(q-1)}{2d}} \right\} \left\{ G_{-\frac{(2d-4)(q-1)}{2(d-1)}} G_{-\frac{2d(q-1)}{2(d-1)}} \right\}. \quad (5.2.12)$$

We use (5.2.12) and Lemma 1.3.12 in (5.2.11), and then simplify to get

$$\begin{aligned}
B &= \frac{q^2 T^{\frac{(3d-1)(q-1)}{3d}} (-1) T^{\frac{q-1}{2}} (-1)}{(q-1) G_{\frac{q-1}{2}}} \sum_{l=0}^{q-2} \begin{pmatrix} T^{l+\frac{q-1}{2}} \\ T^l \end{pmatrix} G_{\frac{q-1}{2}} \begin{pmatrix} T^{l+\frac{(q-1)}{d}} \\ T^{l+\frac{q-1}{d-1}} \end{pmatrix} G_{-\frac{q-1}{d(d-1)}} \cdots \\
&\quad \times \begin{pmatrix} T^{l+\frac{(d-1)(q-1)}{2d}} \\ T^{l+\frac{(d-1)(q-1)}{2(d-1)}} \end{pmatrix} G_{-\frac{(d-2)(q-1)}{2d(d-1)}} \begin{pmatrix} T^{l+\frac{(d+1)(q-1)}{2d}} \\ T^{l+\frac{(d-1)(q-1)}{2(d-1)}} \end{pmatrix} G_{\frac{(d-2)(q-1)}{2d(d-1)}} \cdots \\
&\quad \times \begin{pmatrix} T^{l+\frac{(d-1)(q-1)}{d}} \\ T^{l+\frac{(d-2)(q-1)}{d-1}} \end{pmatrix} G_{\frac{q-1}{d(d-1)}} T^l(-\beta) - T^{\frac{q-1}{2}}(-ad) + 1 \\
&= 1 - \phi(-ad) + q^{\frac{d+1}{2}} {}_dF_{d-1} \left( \begin{matrix} \phi, \chi, \dots, \chi^{\frac{d-1}{2}}, \chi^{\frac{d+1}{2}}, \dots, \chi^{d-1} \\ \psi, \dots, \psi^{\frac{d-1}{2}}, \psi^{\frac{d-1}{2}}, \dots, \psi^{d-2} \end{matrix} \mid -\beta \right).
\end{aligned}$$

Finally, putting the value of  $B$  in (5.2.10), we have

$$\begin{aligned}
q \cdot N_d &= q - \phi(-ad) + q^{\frac{d+1}{2}} \phi(-1) \times \\
&\quad {}_dF_{d-1} \left( \begin{matrix} \phi, \chi, \dots, \chi^{\frac{d-1}{2}}, \chi^{\frac{d+1}{2}}, \dots, \chi^{d-1} \\ \psi, \dots, \psi^{\frac{d-1}{2}}, \psi^{\frac{d-1}{2}}, \dots, \psi^{d-2} \end{matrix} \mid -\beta \right).
\end{aligned}$$

Thus we complete the proof of the theorem.  $\square$

We have the following immediate consequence from our main results.

**Corollary 5.2.4.** *Let  $a, b \in \mathbb{F}_q^\times$  and  $q \equiv 1 \pmod{6}$ . The polynomial  $x^3 + ax + b$  is irreducible over  $\mathbb{F}_q$  if and only if*

$$q^2 \cdot {}_3F_2 \left( \begin{matrix} \phi, \chi_3, \chi_3^2 \\ \phi, \phi \end{matrix} \mid -\frac{27b^2}{4a^3} \right) = \phi(3a) - q\phi(-1),$$

where  $\chi_3$  is a character on  $\mathbb{F}_q$  of order 3.

Again the polynomial  $P_d$  is of degree  $d$ , so it can have at most  $d$  zeros in  $\mathbb{F}_q$ . Thus  $0 \leq N_d \leq d$ , and hence we have the following two corollaries from our main results.

**Corollary 5.2.5.** *Let  $d \geq 2$  be an even integer and  $q \equiv 1 \pmod{d(d-1)}$ . If*

$a, b \in \mathbb{F}_q^\times$ , then

$$\begin{aligned} & \frac{-1}{q^{\frac{d-2}{2}}} \leq \\ & {}_{d-1}F_{d-2} \left( \begin{matrix} \phi, \chi, \dots, \chi^{\frac{d-2}{2}}, \chi^{\frac{d+2}{2}}, \dots, \chi^{d-1} \\ \psi, \dots, \psi^{\frac{d-2}{2}}, \psi^{\frac{d}{2}}, \dots, \psi^{d-2} \end{matrix} \mid \frac{d}{a} \left( \frac{bd}{a(d-1)} \right)^{d-1} \right) \\ & \leq \frac{d-1}{q^{\frac{d-2}{2}}}, \end{aligned}$$

where  $\psi$  and  $\chi$  are characters of order  $d-1$  and  $d$ , respectively.

**Corollary 5.2.6.** *Let  $d > 2$  be an odd integer and  $q \equiv 1 \pmod{d(d-1)}$ . If  $a, b \in \mathbb{F}_q^\times$ ,*

*then*

$$\begin{aligned} & \frac{\phi(ad) - q\phi(-1)}{q^{\frac{d+1}{2}}} \leq \\ & {}_dF_{d-1} \left( \begin{matrix} \phi, \chi, \dots, \chi^{\frac{d-1}{2}}, \chi^{\frac{d+1}{2}}, \dots, \chi^{d-1} \\ \psi, \dots, \psi^{\frac{d-1}{2}}, \psi^{\frac{d-1}{2}}, \dots, \psi^{d-2} \end{matrix} \mid -\frac{d}{a} \left( \frac{bd}{a(d-1)} \right)^{d-1} \right) \\ & \leq \frac{q(d-1)\phi(-1) + \phi(ad)}{q^{\frac{d+1}{2}}}, \end{aligned}$$

where  $\psi$  and  $\chi$  are characters of order  $d-1$  and  $d$ , respectively.

# Chapter 6

## Special Values of Gaussian Hypergeometric Series

### 6.1 Introduction

Classical hypergeometric functions are well understood. Mathematicians such as Gauss, Kummer, Pfaff, and Vandermonde deduced many special values of classical hypergeometric series at different arguments, for example see [4, 5, 17]. Since the introduction of hypergeometric functions over finite fields analogous to classical hypergeometric series, mathematicians are taking interest in finding special values of Gaussian hypergeometric functions. The Gaussian hypergeometric functions are closely related to different parameters of algebraic varieties and number theoretical objects similarly as classical hypergeometric series. However, only a few special values of the Gaussian hypergeometric series are known.

For a given elliptic curve  $E$  over  $\mathbb{Q}$ , the trace of Frobenius endomorphism  $a_p$  are important quantities. Recall that  $\Delta(E)$  denotes the discriminant of  $E$ , and a prime  $p$  is called good or bad accordingly  $p \nmid \Delta(E)$  or  $p \mid \Delta(E)$ . In terms of the trace of Frobenius, the Hasse-Weil  $L$ -function of an elliptic  $E$  is defined by the Euler product

---

<sup>5</sup>The contents of this chapter have been published in *Int. J. Number Theory* (2012) and *J. Number Theory* (2013).

as

$$L(E, s) := \prod_{p|\Delta(E)} (1 - a_p p^{-s})^{-1} \prod_{p \nmid \Delta(E)} (1 - a_p p^{-s} + p^{1-2s})^{-1}, \quad (6.1.1)$$

where  $s$  is a complex number. It is known from Hasse-Weil bound that  $|a_p| < 2\sqrt{p}$ . The Euler product (6.1.1) converges for  $\operatorname{Re}(s) > \frac{3}{2}$  and has analytic continuation to the whole complex plane. Moreover, the Birch and Swinnerton-Dyer conjecture concerns the behavior of  $L(E, s)$  at  $s = 1$ . In fact, the conjecture predicts that  $\operatorname{ord}_{s=1}(L(E, s)) = \operatorname{rank}(E/\mathbb{Q})$ .

In Chapter 2, we have found general formulas for the trace of Frobenius endomorphism of certain families of elliptic curves in Weierstrass normal form in terms of Gaussian hypergeometric series. Thus, finding special values of Gaussian hypergeometric functions is an important and interesting problem. Earlier works of Greene [18], Ono [34], Ahlgren-Ono [1], and Evans-Greene [11, 12] pave the way to find special values of many Gaussian hypergeometric functions. Most of them have been used to solve many old conjectures [31, 32] and supercongruences [33].

In this chapter, we mainly concentrate to find special values of certain Gaussian hypergeometric series using our earlier results.

## 6.2 Main results

In this section, we give a brief description of the special values of Gaussian hypergeometric series those have been already evaluated. Then we deduce some more values of hypergeometric functions over finite fields. We start with the special values of  ${}_2F_1$  Gaussian hypergeometric series.

### 6.2.1 Values of ${}_2F_1$ Gaussian hypergeometric series

The story of special values of Gaussian hypergeometric series begins from its inception in [18] by Greene. After introducing hypergeometric functions over finite fields,

Greene [18] deduced certain special values of  ${}_2F_1$  Gaussian hypergeometric functions at some particular arguments.

**Theorem 6.2.1.** [18, (4.11), (4.14) & (4.15)] *For any two characters  $A, B$  on  $\mathbb{F}_q$ , we have*

$$\begin{aligned} (i) \quad {}_2F_1 \left( \begin{matrix} A, & B \\ & \overline{AB} \end{matrix} \middle| -1 \right) &= \begin{cases} 0, & \text{if } B \text{ is not a square;} \\ \binom{C}{A} + (\phi_A^C), & \text{if } B = C^2. \end{cases} \\ (ii) \quad {}_2F_1 \left( \begin{matrix} A, & B \\ & A^2 \end{matrix} \middle| 2 \right) &= A(-1) \begin{cases} 0, & \text{if } B \text{ is not a square;} \\ \binom{C}{A} + (\phi_A^C), & \text{if } B = C^2. \end{cases} \\ (iii) \quad {}_2F_1 \left( \begin{matrix} A, & \overline{A} \\ & \overline{AB} \end{matrix} \middle| \frac{1}{2} \right) &= A(-2) \begin{cases} 0, & \text{if } B \text{ is not a square;} \\ \binom{C}{A} + (\phi_A^C), & \text{if } B = C^2. \end{cases} \end{aligned}$$

Further, Ono worked in this direction and found the following interesting results in which he explicitly deduced special values of  ${}_2F_1$  hypergeometric series over  $\mathbb{F}_p$ . He used the technique of complex multiplication of elliptic curves to establish these results.

**Theorem 6.2.2.** [34, Thm. 2] *Let  $\lambda \in \{-1, \frac{1}{2}, 2\}$ . If  $p$  is an odd prime, then*

$${}_2F_1 \left( \begin{matrix} \phi, & \phi \\ & \varepsilon \end{matrix} \middle| \lambda \right) = \begin{cases} 0, & \text{if } p \equiv 3 \pmod{4}; \\ \frac{2x(-1)^{\frac{x+y+1}{2}}}{p}, & \text{if } x^2 + y^2 = p \equiv 1 \pmod{4}, \text{ and } x \text{ odd.} \end{cases}$$

Motivated by all these results, we have also deduced certain special values of  ${}_2F_1$  Gaussian hypergeometric series. We have mainly used the formulas of traces of Frobenius of elliptic curves and some transformation formulas of Gaussian hypergeometric series to prove the results.

**Theorem 6.2.3.** *Let  $q = p^e$ ,  $p > 0$  a prime with  $q \equiv 1 \pmod{4}$ . Then*

$$\begin{aligned}
(i) \quad {}_2F_1 \left( \begin{matrix} \chi_4, & \chi_4^3 \\ & \varepsilon \end{matrix} \middle| \frac{1}{9} \right) &= \chi_4(-1)\phi(3) \left[ \binom{\chi_4}{\phi} + \binom{\chi_4^3}{\phi} \right]. \\
(ii) \quad {}_2F_1 \left( \begin{matrix} \chi_4, & \chi_4^3 \\ & \varepsilon \end{matrix} \middle| \frac{8}{9} \right) &= \phi(3) \left[ \binom{\chi_4}{\phi} + \binom{\chi_4^3}{\phi} \right]. \\
(iii) \quad {}_2F_1 \left( \begin{matrix} \chi_4, & \chi_4 \\ & \varepsilon \end{matrix} \middle| -\frac{1}{8} \right) &= \chi_4(-8) \left[ \binom{\chi_4}{\phi} + \binom{\chi_4^3}{\phi} \right]. \\
(iv) \quad {}_2F_1 \left( \begin{matrix} \chi_4, & \chi_4 \\ & \varepsilon \end{matrix} \middle| -8 \right) &= \left[ \binom{\chi_4}{\phi} + \binom{\chi_4^3}{\phi} \right].
\end{aligned}$$

where  $\chi_4$  is a character of order 4 on  $\mathbb{F}_q$ .

*Proof.* If we put  $A = B = \phi$  in Theorem 6.2.1 (iii) we obtain

$$\begin{aligned}
{}_2F_1 \left( \begin{matrix} \phi, & \phi \\ & \varepsilon \end{matrix} \middle| \frac{1}{2} \right) &= \phi(-2) \begin{cases} 0, & \text{if } q \equiv 3 \pmod{4}; \\ \left[ \binom{\chi_4}{\phi} + \binom{\phi\chi_4}{\phi} \right], & \text{if } q \equiv 1 \pmod{4}, \end{cases} \\
&= \begin{cases} 0, & \text{if } q \equiv 3 \pmod{4}; \\ \phi(2) \left[ \binom{\chi_4}{\phi} + \binom{\chi_4^3}{\phi} \right], & \text{if } q \equiv 1 \pmod{4}, \end{cases} \quad (6.2.1)
\end{aligned}$$

This is because any character  $\chi$  of order  $l$  on  $\mathbb{F}_q$  is square if and only if  $\frac{q-1}{l}$  is even and hence  $\phi = \chi_4^2$ .

(i) Replacing  $\alpha$  by 6 in Corollary 2.3.3, we have

$${}_2F_1 \left( \begin{matrix} \chi_4, & \chi_4^3 \\ & \varepsilon \end{matrix} \middle| \frac{1}{9} \right) = \chi_4(-1)\phi(6) {}_2F_1 \left( \begin{matrix} \phi, & \phi \\ & \varepsilon \end{matrix} \middle| \frac{1}{2} \right)$$

Hence the proof follows from (6.2.1).

(ii) Putting  $x = \frac{8}{9}$  in Theorem 1.3.15 (i), we obtain

$${}_2F_1 \left( \begin{matrix} \chi_4, & \chi_4^3 \\ & \varepsilon \end{matrix} \middle| \frac{8}{9} \right) = \chi_4(-1) {}_2F_1 \left( \begin{matrix} \chi_4, & \chi_4^3 \\ & \varepsilon \end{matrix} \middle| \frac{1}{9} \right).$$



Thus the result (i) completes the proof of (ii).

(iii) For  $x = -\frac{1}{8}$ , Theorem 1.3.15 (ii) yields

$${}_2F_1 \left( \begin{matrix} \chi_4, & \chi_4 & | & -\frac{1}{8} \\ \epsilon & & & \end{matrix} \right) = \chi_4^3 \left( \frac{9}{8} \right) {}_2F_1 \left( \begin{matrix} \chi_4, & \chi_4^3 & | & \frac{1}{9} \\ \epsilon & & & \end{matrix} \right)$$

Hence the proof of (iii) follows from the proof of (i).

(iv) Finally, putting  $x = -8$  in Theorem 1.3.15 (ii), we have

$${}_2F_1 \left( \begin{matrix} \chi_4, & \chi_4 & | & -8 \\ \epsilon & & & \end{matrix} \right) = \chi_4^3(9) {}_2F_1 \left( \begin{matrix} \chi_4, & \chi_4^3 & | & \frac{8}{9} \\ \epsilon & & & \end{matrix} \right)$$

This completes the proof due to (ii).  $\square$

Moreover, if we use Theorem 1.3.15 (i) in each of Theorem 6.2.3 (iii) & (iv), respectively we can deduce the following Corollary.

**Corollary 6.2.4.** *Let  $q = p^e$ ,  $p > 0$  a prime and  $q \equiv 1 \pmod{4}$ . Then*

$$\begin{aligned} (i) \quad {}_2F_1 \left( \begin{matrix} \chi_4, & \chi_4 & | & \frac{9}{8} \\ \epsilon & & & \end{matrix} \right) &= \chi_4(8) \left[ \binom{\chi_4}{\phi} + \binom{\chi_4^3}{\phi} \right]. \\ (ii) \quad {}_2F_1 \left( \begin{matrix} \chi_4, & \chi_4 & | & 9 \\ \epsilon & & & \end{matrix} \right) &= \chi_4(-1) \left[ \binom{\chi_4}{\phi} + \binom{\chi_4^3}{\phi} \right]. \end{aligned}$$

where  $\chi_4$  is a character of order 4 on  $\mathbb{F}_q$ .

The above special values of Gaussian hypergeometric functions are valid only for certain special characters of particular order in  $\mathbb{F}_q$ . we now focus on special values of hypergeometric functions over finite fields containing characters of arbitrary order.

**Theorem 6.2.5.** *Let  $S$  be a character on  $\mathbb{F}_q$  whose order is not equal to 3. If  $S$  is*

square of some character on  $\mathbb{F}_q$ , then

$$\begin{aligned}
(i) \quad {}_2F_1 \left( \begin{matrix} \sqrt{S^{-3}}\phi, & \sqrt{S^{-3}} \\ & S^{-2} \end{matrix} \middle| \frac{4}{3} \right) &= \begin{cases} 0, & \text{if } q \equiv 2 \pmod{3}; \\ \frac{S(\frac{8}{27})J(\sqrt{S^{-1}}, \sqrt{S^3}\phi)}{J(\phi, S)} \left[ \binom{S}{\chi_3} + \binom{S}{\chi_3^2} \right], & \text{if } q \equiv 1 \pmod{3}. \end{cases} \\
(ii) \quad {}_2F_1 \left( \begin{matrix} \sqrt{S^{-3}}\phi, & \sqrt{S^{-3}} \\ & S^{-1}\phi \end{matrix} \middle| -\frac{1}{3} \right) &= \begin{cases} 0, & \text{if } q \equiv 2 \pmod{3}; \\ \frac{S(\frac{8}{27})J(\sqrt{S^{-1}}, \sqrt{S^3}\phi)}{\sqrt{S}\phi(-1)J(\phi, S)} \left[ \binom{S}{\chi_3} + \binom{S}{\chi_3^2} \right], & \text{if } q \equiv 1 \pmod{3}. \end{cases} \\
(iii) \quad {}_2F_1 \left( \begin{matrix} \sqrt{S^{-3}}\phi, & \sqrt{S^{-1}} \\ & S^{-2} \end{matrix} \middle| 4 \right) &= \begin{cases} 0, & \text{if } q \equiv 2 \pmod{3}; \\ \frac{\sqrt{S}(-\frac{64}{27})J(\sqrt{S^{-1}}, \sqrt{S^3}\phi)}{\phi(-3)J(\phi, S)} \left[ \binom{S}{\chi_3} + \binom{S}{\chi_3^2} \right], & \text{if } q \equiv 1 \pmod{3} \text{ and } S \neq \phi. \end{cases} \\
(iv) \quad {}_2F_1 \left( \begin{matrix} \sqrt{S^{-3}}\phi, & \sqrt{S}\phi \\ & S^{-1}\phi \end{matrix} \middle| \frac{1}{4} \right) &= \begin{cases} 0, & \text{if } q \equiv 2 \pmod{3}; \\ \frac{\sqrt{S}(-\frac{1}{27})J(\sqrt{S^{-1}}, \sqrt{S^3}\phi)}{\phi(3)J(\phi, S)} \left[ \binom{S}{\chi_3} + \binom{S}{\chi_3^2} \right], & \text{if } q \equiv 1 \pmod{3}. \end{cases}
\end{aligned}$$

We need the following two corollaries to deduce the above special values.

**Lemma 6.2.6.** *Let  $S$  be any character on  $\mathbb{F}_q$ . For  $\lambda = \frac{1}{3}$ , we have*

$$\sum_{x \in \mathbb{F}_q} S((x-1)(x^2 + \lambda)) = \begin{cases} 0, & \text{if } q \equiv 2 \pmod{3}; \\ qS(-\frac{8}{27}) \left[ \binom{S}{\chi_3} + \binom{S}{\chi_3^2} \right], & \text{if } q \equiv 1 \pmod{3}, \end{cases}$$

where  $\chi_3$  is a character of order 3 on  $\mathbb{F}_q$ .

*Proof.* Recall that making the change of variables  $(x, y) \rightarrow (\frac{x}{9} + \frac{1}{3}, y)$ , and then replacing  $-\frac{x}{6}$  by  $x$  we obtain the equivalent form of

$$y^l = (x-1)(x^2 + \frac{1}{3})$$

as

$$y^l = -\frac{8}{27}(1+x^3).$$

For any multiplicative character  $A$  on  $\mathbb{F}_q$ , we have the binomial theorem from [18] as

$$A(1+x) = \delta(x) + \frac{q}{q-1} \sum_{\chi} \binom{A}{\chi} \chi(x),$$

where  $\delta(x) = 1$  (resp.  $0$ ) if  $x = 0$  (resp.  $x \neq 0$ ). Using this, we have

$$\begin{aligned} \sum_{x \in \mathbb{F}_q} S((x-1)(x^2 + \frac{1}{3})) &= \sum_{x \in \mathbb{F}_q} S(-\frac{8}{27}) S(1+x^3) \\ &= S(-\frac{8}{27}) + \frac{q}{q-1} S(-\frac{8}{27}) \sum_{x \in \mathbb{F}_q} \sum_{\chi} \binom{S}{\chi} \chi^3(x) \\ &= S(-\frac{8}{27}) + \frac{q}{q-1} S(-\frac{8}{27}) \sum_{\chi} \binom{S}{\chi} \sum_{x \in \mathbb{F}_q} \chi^3(x). \end{aligned}$$

By Lemma 1.3.7, the innermost sum in the second term is nonzero only if  $\chi^3 = \varepsilon$  at which it is  $q-1$ . Thus  $\chi = \varepsilon$ , if  $q \equiv 2 \pmod{3}$ ; and  $\chi = \varepsilon, \chi_3$ , or  $\chi_3^2$ , if  $q \equiv 1 \pmod{3}$ . Hence the result follows immediately.  $\square$

**Lemma 6.2.7.** *If  $S$  is square of some character on  $\mathbb{F}_q$  and  $S$  is not of order 3, then*

$$\sum_{x \in \mathbb{F}_q} S((x-1)(x^2 + \lambda)) = \frac{qJ(\phi, S)}{J(\sqrt{S^{-1}}, \sqrt{S^3}\phi)} \cdot {}_2F_1 \left( \begin{matrix} \sqrt{S^{-3}}\phi, & \sqrt{S^{-3}} \\ & S^{-2} \end{matrix} \middle| 1 + \lambda \right)$$

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

$$\sum_{x \in \mathbb{F}_q} S((x-1)(x^2 + \lambda)) = S(-\lambda)g(S, S; -\frac{1}{\lambda}).$$

Again,  $S$  is a square of some character of  $\mathbb{F}_q$ . Hence applying Theorem 4.2.1, we deduce that

$$g(S, S; -\frac{1}{\lambda}) = qS^3(2)S(-\frac{1}{\lambda})F^*(S^{-3}, S^{-2}; 1 + \lambda),$$

and hence

$$\sum_{x \in \mathbb{F}_q} S((x-1)(x^2 + \lambda)) = qS^3(2)F^*(S^{-3}, S^{-2}; 1 + \lambda). \quad (6.2.2)$$

Further,  $S$  is not of order 3. Thus using Theorem 4.2.3, we complete the proof.  $\square$

Following the proof of Lemma 6.2.7 and applying Proposition 4.2.4 in spite of Theorem 4.2.3 in (6.2.2), we have the following result.

**Lemma 6.2.8.** *If  $S$  is a character of order 3 on  $\mathbb{F}_q$ , then*

$$\sum_{x \in \mathbb{F}_q} S((x-1)(x^2 + \lambda)) = q \cdot {}_2F_1 \left( \begin{matrix} \phi, & \varepsilon \\ & S \end{matrix} \middle| x \right). \quad (6.2.3)$$

Now, we give the proof of Theorem 6.2.5 using Lemma 6.2.6 and Lemma 6.2.7.

**Proof of 6.2.5.** (i) Putting  $\lambda = \frac{1}{3}$  in Lemma 6.2.7, we have

$${}_2F_1 \left( \begin{matrix} \sqrt{S^{-3}}\phi, & \sqrt{S^{-3}} \\ & S^{-2} \end{matrix} \middle| \frac{4}{3} \right) = \frac{J(\sqrt{S^{-1}}, \sqrt{S^3}\phi)}{qJ(\phi, S)} \sum_{x \in \mathbb{F}_q} S((x-1)(x^2 + \frac{1}{3})).$$

Therefore, we complete the proof of (i) after using Lemma 6.2.6.

(ii) Taking  $x = \frac{4}{3}$  in Theorem 1.3.15 (i), we obtain

$${}_2F_1 \left( \begin{matrix} \sqrt{S^{-3}}\phi, & \sqrt{S^{-3}} \\ & S^{-1}\phi \end{matrix} \middle| -\frac{1}{3} \right) = \sqrt{S}\phi(-1) {}_2F_1 \left( \begin{matrix} \sqrt{S^{-3}}\phi, & \sqrt{S^{-3}} \\ & S^{-2} \end{matrix} \middle| \frac{4}{3} \right).$$

Now using (i), we complete the proof.

(iii) Applying Theorem 1.3.15 (ii) for  $x = \frac{4}{3}$ , we have

$${}_2F_1 \left( \begin{matrix} \sqrt{S^{-3}}\phi, & \sqrt{S^{-1}} \\ & S^{-2} \end{matrix} \middle| 4 \right) = \sqrt{S^3}\phi(-3) {}_2F_1 \left( \begin{matrix} \sqrt{S^{-3}}\phi, & \sqrt{S^{-3}} \\ & S^{-2} \end{matrix} \middle| \frac{4}{3} \right),$$

if  $S \neq \phi$ . Hence the result follows from (i).

(iv) Using Theorem 1.3.15 (ii) for  $x = -\frac{1}{3}$ , we find that

$${}_2F_1 \left( \begin{matrix} \sqrt{S^{-3}}\phi, & \sqrt{S}\phi \\ & S^{-1}\phi \end{matrix} \middle| \frac{1}{4} \right) = \phi(-1)\sqrt{S^3}\phi\left(\frac{3}{4}\right) {}_2F_1 \left( \begin{matrix} \sqrt{S^{-3}}\phi, & \sqrt{S^{-3}} \\ & S^{-1}\phi \end{matrix} \middle| -\frac{1}{3} \right)$$

and then the proof follows from the proof of (ii).  $\square$

## 6.2.2 Values of ${}_3F_2$ Gaussian hypergeometric series

The value of  ${}_3F_2$  Gaussian hypergeometric series at the argument 1 is first evaluated by Greene in his famous paper [18]. The non-trivial values of  ${}_3F_2$  hypergeometric

series over  $\mathbb{F}_p$  are explicitly deduced by Ono. He used the technique of complex multiplication of elliptic curves to deduce the following special values of  ${}_3F_2$  Gaussian hypergeometric series.

**Theorem 6.2.9.** [34, Thm. 6] *If  $\lambda \in \{\frac{9}{2}, 36, 8, 3, -12, \frac{63}{16}, -252\}$ , then for every odd prime  $p$  for which  $\text{ord}_p(\lambda(\lambda - 4)) = 0$ , the value of  ${}_3F_2(\frac{4}{4-\lambda})$  is given by:*

$$\begin{aligned}
(i) \quad {}_3F_2 \left( \begin{matrix} \phi, \phi, \phi \\ \varepsilon, \varepsilon \end{matrix} \middle| -8 \right) &= \begin{cases} -\frac{1}{p}, & \text{if } p \equiv 3 \pmod{4}; \\ \frac{4x^2-p}{p^2}, & \text{if } p \equiv 1 \pmod{4}, p = x^2 + y^2, \text{ and } x \text{ odd.} \end{cases} \\
(ii) \quad {}_3F_2 \left( \begin{matrix} \phi, \phi, \phi \\ \varepsilon, \varepsilon \end{matrix} \middle| -\frac{1}{8} \right) &= \begin{cases} -\frac{\phi(2)}{p}, & \text{if } p \equiv 3 \pmod{4}; \\ \frac{\phi(2)(4x^2-p)}{p^2}, & \text{if } x^2 + y^2 = p \equiv 1 \pmod{4} \text{ and } x \text{ odd.} \end{cases} \\
(iii) \quad {}_3F_2 \left( \begin{matrix} \phi, \phi, \phi \\ \varepsilon, \varepsilon \end{matrix} \middle| -1 \right) &= \begin{cases} -\frac{\phi(2)}{p}, & \text{if } p \equiv 5, 7 \pmod{8}; \\ \frac{\phi(2)(4x^2-p)}{p^2}, & \text{if } p \equiv 1, 3 \pmod{8}, p = x^2 + 2y^2. \end{cases} \\
(iv) \quad {}_3F_2 \left( \begin{matrix} \phi, \phi, \phi \\ \varepsilon, \varepsilon \end{matrix} \middle| 4 \right) &= \begin{cases} -\frac{\phi(-3)}{p}, & \text{if } p \equiv 2 \pmod{3}; \\ \frac{\phi(-3)(4x^2-p)}{p^2}, & \text{if } p \equiv 1 \pmod{3}, p = x^2 + 3y^2. \end{cases} \\
(v) \quad {}_3F_2 \left( \begin{matrix} \phi, \phi, \phi \\ \varepsilon, \varepsilon \end{matrix} \middle| \frac{1}{4} \right) &= \begin{cases} -\frac{\phi(3)}{p}, & \text{if } p \equiv 2 \pmod{3}; \\ \frac{\phi(3)(4x^2-p)}{p^2}, & \text{if } p \equiv 1 \pmod{3}, p = x^2 + 3y^2. \end{cases} \\
(vi) \quad {}_3F_2 \left( \begin{matrix} \phi, \phi, \phi \\ \varepsilon, \varepsilon \end{matrix} \middle| 64 \right) &= \begin{cases} -\frac{\phi(-7)}{p}, & \text{if } p \equiv 3, 5, 6 \pmod{7}; \\ \frac{\phi(-7)(4x^2-p)}{p^2}, & \text{if } p \equiv 1, 2, 4 \pmod{7}, p = x^2 + 7y^2. \end{cases} \\
(vii) \quad {}_3F_2 \left( \begin{matrix} \phi, \phi, \phi \\ \varepsilon, \varepsilon \end{matrix} \middle| \frac{1}{64} \right) &= \begin{cases} -\frac{\phi(7)}{p}, & \text{if } p \equiv 3, 5, 6 \pmod{7}; \\ \frac{\phi(7)(4x^2-p)}{p^2}, & \text{if } p \equiv 1, 2, 4 \pmod{7}, p = x^2 + 7y^2. \end{cases}
\end{aligned}$$

The characters involve in the above formulas are only quadratic and trivial. In [11], Evans and Greene gave an expression for  ${}_3F_2(\frac{1}{4})$  containing characters of arbitrary orders, which extend Theorem 6.2.9 (v) evaluated by Ono. To obtain the following result, Evans and Greene deduced some transformation relations between  ${}_3F_2$  and  ${}_2F_1$  hypergeometric functions over finite fields analogous to Clausen Theorem of classical hypergeometric series.

**Theorem 6.2.10.** [11, Thm. 1.3] *Let  $S$  be a character on  $\mathbb{F}_q$  which is not trivial, cubic, or quartic. Then*

$${}_3F_2 \left( \begin{matrix} \bar{S}, & S^3, & S \\ & S^2, & S\phi \end{matrix} \middle| \frac{1}{4} \right) = \begin{cases} \frac{\phi(-1)S(4)}{q}, & \text{if } q \equiv 2 \pmod{3}; \\ \frac{\phi(-1)S(4)}{q} \left( 1 + \frac{J(S,\chi)}{J(S,\bar{\chi})} + \frac{J(S,\bar{\chi})}{J(S,\chi)} \right), & \text{if } q \equiv 1 \pmod{3}, \end{cases}$$

where  $\chi$  is a character of order 3 on  $\mathbb{F}_q$ .

Further, Evans and Greene deduced the following special value of Gaussian hypergeometric series.

**Theorem 6.2.11.** [12, Thm. 1.8] *Suppose that  $S$  is a character whose order is not equal to 1, 3 or 4 over  $\mathbb{F}_q$ . Then*

$${}_3F_2 \left( \begin{matrix} \bar{S}, & S^3, & S \\ & S^2, & S\phi \end{matrix} \middle| -\frac{1}{8} \right) = \begin{cases} \frac{-\phi(-1)S(-8)}{q}, & \text{if } S \text{ is not a square;} \\ \frac{\phi(-1)S(8)}{q} + \frac{\phi(-1)S(2)J(\bar{S},S^3)}{q^2J(S,S)} (J(S,D)^2 + J(S,D\phi)^2), & \text{if } S = D^2. \end{cases}$$

In the following theorem, we evaluate the value of  ${}_3F_2(4)$  hypergeometric series over  $\mathbb{F}_q$ , which extends another result of Ono [34] (see Theorem 6.2.9 (vi)). The result of Ono can be obtained by putting  $S = \phi$ , thus solving a problem posed by M. Koike [25, p. 465].

**Theorem 6.2.12.** *If  $S$  is a character on  $\mathbb{F}_q$  with order not equal to 1, 3, or 4, then*

$${}_3F_2 \left( \begin{matrix} S^{-3}, & S^{-1}, & S^{-2}\phi \\ & S^{-4}, & S^{-2} \end{matrix} \middle| 4 \right) = \begin{cases} \frac{\phi(-3)S(16)}{q}, & \text{if } q \equiv 2 \pmod{3}; \\ \frac{S(-\frac{16}{27})^q J(S^{-1}, S^{-1})}{J(S^{-3}, S)} \left[ \binom{S}{\chi_3} + \binom{S}{\chi_3^2} \right]^2 \\ \frac{\phi(-3)S(16)}{q}, & \text{if } q \equiv 1 \pmod{3}, \end{cases}$$

where  $\chi_3$  is a character of order 3 of  $\mathbb{F}_q$ .

We remark that in view of Theorem 1.3.14, there is a result similar to Theorem 6.2.12 in which the argument 4 is replaced by  $\frac{1}{4}$ . However, our result about  ${}_3F_2(\frac{1}{4})$

will be different from Theorem 6.2.10 obtained by Evans and Greene. We now prove the following lemma from which Theorem 6.2.12 will follow directly after combining with Lemma 6.2.6.

**Lemma 6.2.13.** *If  $S$  is a character on  $\mathbb{F}_q$  whose order is not equal to 1, 3 or 4, then*

$${}_3F_2 \left( \begin{matrix} S^{-3}, & S^{-1}, & S^{-2}\phi \\ & S^{-4}, & S^{-2} \end{matrix} \middle| \frac{1+\lambda}{\lambda} \right) = \frac{J(S^{-1}, S^{-1})}{q^2 S(-4\lambda^3) J(S^{-3}, S)} \times \left[ \sum_{x \in \mathbb{F}_q} S((x-1)(x^2+\lambda)) \right]^2 - \frac{S^2(\frac{1+\lambda}{\lambda})}{q} \phi(-\lambda).$$

*Proof.* Since  $S$  is a character on  $\mathbb{F}_q$  whose order is not equal to 1, 3 or 4, so applying Theorem 4.2.2 directly for  $A = S^{-3}$ ,  $C = S^{-2}$ , and  $x = \frac{1+\lambda}{\lambda}$ , we obtain

$${}_3F_2 \left( \begin{matrix} S^{-3}, & S^{-1}, & S^{-2}\phi \\ & S^{-4}, & S^{-2} \end{matrix} \middle| \frac{1+\lambda}{\lambda} \right) = \frac{J(S^{-1}, S^{-1})}{q^2 S(-4\lambda) J(S^{-3}, S)} g(S, S; -\frac{1}{\lambda})^2 - \frac{S^2(\frac{1+\lambda}{\lambda})}{q} \phi(-\lambda). \quad (6.2.4)$$

Again, from (4.2.3), we have

$$g(S, S; -\frac{1}{\lambda}) = \sum_{x \in \mathbb{F}_q} S^{-1}(-\lambda) S((x-1)(x^2+\lambda)). \quad (6.2.5)$$

Hence combining (6.2.4) and (6.2.5), we complete the proof.  $\square$

**Proof of 6.2.12.** Putting  $\lambda = \frac{1}{3}$  in Lemma 6.2.13, we obtain

$${}_3F_2 \left( \begin{matrix} S^{-3}, & S^{-1}, & S^{-2}\phi \\ & S^{-4}, & S^{-2} \end{matrix} \middle| 4 \right) = \frac{J(S^{-1}, S^{-1})}{q^2 S(-\frac{4}{27}) J(S^{-3}, S)} \left[ \sum_{x \in \mathbb{F}_q} S((x-1)(x^2 + \frac{1}{3})) \right]^2 - \frac{S(16)}{q} \phi(-3).$$

Now combining this with Lemma 6.2.6, we complete the proof of the result.  $\square$

# Bibliography

- [1] Ahlgren, S. & Ono, K. A Gaussian hypergeometric series and Apéry number congruences, *J. Reine Angew. Math.* **518**, 187–212, 2000.
- [2] Ahlgren, S. The points of a certain fivefold over finite fields and twelfth power of the eta function, *Finite Fields Appl.* **8**(1), 18–33, 2002.
- [3] Ahlgren, S. & Ono, K. Modularity of certain Calabi-Yau threefold, *Monatsh Math.* **129**(3), 177–190, 2000.
- [4] Andrews, G. E., et al. *Special functions*, Encyclopedia of Mathematics and its Application, 71<sup>th</sup> ed., Cambridge Univ. Press, Cambridge, 1999.
- [5] Bailey, W. *Generalized hypergeometric series*, Cambridge Univ. Press, Cambridge, 1935.
- [6] Berndt, B. C., et al. *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, A Wiley-Interscience Publication, New York, 1997.
- [7] Bernstein, D. J., Birkner, P., Joye, M., Lange, T., & Peters, C. Twisted Edwards curves, in *Africacrypt' 2008*, Springer-Verlag, LNCS **5023**, 389–405.
- [8] Beukers, F. Algebraic values of G-functions, *J. Reine Angew. Math.* **434**, 45–65, 1993.
- [9] Erdelyi, A., et al. *Higher Transcendental Functions*, McGraw-Hill, New York, 1953.



- [10] Euler, L. *Institutiones Calculi Integralis*, Opera Omnia, 1769.
- [11] Evans, R. & Greene, J. Evaluation of Hypergeometric Functions over Finite Fields, *Hiroshima Math. J.* **39**(2), 217–235, 2009.
- [12] Evans, R. & Greene, J. Clausen Theorem and Hypergeometric Functions over Finite Fields, *Finite Fields Appl.* **15**, 97–109, 2009.
- [13] Farashahi, R. R. On the Number of Distinct Legendre, Jacobi, Hessian and Edwards Curves. <http://arxiv.org/pdf/1112.5714v1.pdf>, 2011.
- [14] Fuselier, J. Hypergeometric functions over  $\mathbb{F}_p$  and relations to elliptic curve and modular forms, *Proc. Amer. Math. Soc.* **138**(1), 109–123, 2010.
- [15] Fuselier, J. Traces of Hecke operators in level 1 and Gaussian hypergeometric functions, *Proc. Amer. Math. Soc.*, **141**(6), 1871–1881, 2013.
- [16] Frechette, S., et al. Gaussian hypergeometric functions and traces of Hecke operators, *Int. Math. Res. Not.* **60**, 3233–3262, 2004.
- [17] Gauss, G. F. Disquisitiones generales circa seriem infinitam, *Comm. Soc. Reg. Gött. II* **3**, 123–162, 1882.
- [18] Greene, J. Hypergeometric functions over finite fields, *Trans. Amer. Math. Soc.* **301**(1), 77–101, 1987.
- [19] Greene, J. Hypergeometric function over finite fields and representation of  $SL(2, q)$ , *Rocky Mountain J. Math.* **23**(2), 547–568, 1993.
- [20] Greene, J. & Stanton, D. A character sum evaluation and Gaussian hypergeometric series, *J. Number Theory* **23**, 136–148, 1986.
- [21] Greene, J. Lagrange inversion over finite fields, *Pacific J. Math.* **130**(2), 547–568, 1987.
- [22] Housemüller, D. *Elliptic Curves*, 2<sup>nd</sup> ed., Graduate Text in Mathematics, Springer, New York, 2002.

- [23] Ireland, K. & Rosen, M. *A Classical Introduction to Modern Number Theory*, 2<sup>nd</sup> ed., Springer International Edition, Springer, 2005.
- [24] Kirwan, F. *Complex algebraic curves*, LMS Student Texts 23, Cambridge University Press, Cambridge, 1992.
- [25] Koike, M. Hypergeometric series over finite fields and Apéry numbers, *Hiroshima Math. J.* **22**, 461–467, 1992.
- [26] Lang, S. *Cyclotomic Fields I and II*, Graduate Texts in Mathematics, Springer-Verlag, New York, 1990.
- [27] Lennon, C. Gaussian hypergeometric evaluations of traces of Frobenius for elliptic curves, *Proc. Amer. Math. Soc.* **139**, 1931–938, 2011.
- [28] Lennon, C. Trace formulas for Hecke operators, Gaussian hypergeometric functions, and the modularity of a threefold, *J. Number Theory* **131**(12), 2320–2351, 2011.
- [29] Lidl, R. & Niederreiter, H. *Finite Fields*, Encyclopedia of mathematics and its applications, 20<sup>th</sup> ed., Cambridge Univ. Press, Cambridge, 2008.
- [30] McCarthy, D.  ${}_3F_2$  Hypergeometric series and periods of elliptic curves, *Int. J. Number Theory* **6**(3), 461–470, 2010.
- [31] Mortenson, E. A supercongruence conjecture of Rodriguez-Villegas for a certain truncated hypergeometric function, *J. Number Theory* **99**(1), 139–147, 2003.
- [32] Mortenson, E. Supercongruences between truncated  ${}_2F_1$  hypergeometric functions and their Gaussian analogs, *Trans. Amer. Math. Soc.* **355**(3), 987–1007, 2003.
- [33] Mortenson, E. Supercongruences for truncated  ${}_{n+1}F_n$  hypergeometric series with applications to certain weight three newforms, *Proc. Amer. Math. Soc.* **133**(2), 321–330, 2005.

- [34] Ono, K. Values of Gaussian hypergeometric series, *Trans. Amer. Math. Soc.* **350**(3), 1205–1223, 1998.
- [35] Ono, K. *The web of modularity: Arithmetic of the Coefficients of Modular Forms and  $q$ -series*, Amer. Math. Soc., Providence, RI, 2004.
- [36] Rouse J. Hypergeometric function and elliptic curves, *Ramanujan J.* **12** (2), 197–205, 2006.
- [37] Silverman, J. H. & Tate, J. *Rational points on elliptic curves*, Springer, New Delhi, 2005.
- [38] Slater, L. J. *Generalized hypergeometric functions*, Cambridge Univ. Press, Cambridge, 1966.
- [39] Stiller, P. F. Classical automorphic forms and hypergeometric functions, *J. Number Theory* **28**(2), 219–232, 1988.
- [40] Vega, M. V. Relations between hypergeometric functions over finite fields and algebraic curves, *Int. J. Number Theory* **7**(8), 2171–2195, 2011.
- [41] Washington, L. C. *Elliptic Curves*, 2<sup>nd</sup> ed., Discrete Mathematics and its applications, Chapman and Hall/CRC, New York, 2003.

# Publications

## List of Publications

1. Barman, R. & Kalita, G. Hypergeometric functions and a family of algebraic curves, *Ramanujan J.* **28**(2), 175–185, 2012.
2. Barman, R. & Kalita, G. Certain values of Gaussian hypergeometric series and a family of algebraic curves, *Int. J. Number Theory* **8**(4), 945–961, 2012.
3. Barman, R. & Kalita, G. Hypergeometric functions over  $\mathbb{F}_q$  and traces of Frobenius for elliptic curves, *Proc. Amer. Math. Soc.* **141**(10), 3403–3410, 2013.
4. Barman, R. & Kalita, G. Elliptic curves and special values of Gaussian hypergeometric series, *J. Number Theory* **133**(9), 3099–3111, 2013.
5. Barman, R. & Kalita, G. On the polynomial  $x^d + ax + b$  over  $\mathbb{F}_q$  and Gaussian hypergeometric series, *Int. J. Number Theory* **9**(7), 1753–1763, 2013.