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 $\,_{2}F_{1}$ 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

\[ \binom{r+1}{F_r} \left( \begin{array}{cccc} a_0, & a_1, & \ldots, & a_r \\ b_1, & \ldots, & b_r \end{array} \right | 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 \(\text{Re}(\sum b_i - \sum a_i) > 0\) and converges conditionally for \(|z| = 1, z \neq 1\) if \(0 \geq \text{Re}(\sum b_i - \sum a_i) > -1\). 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

\[ \frac{\Omega(2E_1)}{\pi} = 2F_1 \left( \begin{array}{c} \frac{1}{2}, \frac{1}{2} \\ 1 \end{array} \right | t \right). \]

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 \(2F_1(\begin{array}{c} \frac{1}{12}, \frac{5}{12} \\ \frac{1}{2} \end{array} | \frac{27}{4} t^2))\).

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 $t > 0$,

$$3F_2\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2} \mid \frac{t}{1+t}\right) = \frac{\sqrt{1+t} \Omega(3E_2)^2}{\pi^2},$$

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 Lagendre’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 $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$ 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

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

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

$$\,_{n+1}F_n\left(\begin{array}{c} A_0, A_1, \ldots, A_n \\ B_1, \ldots, B_n \end{array} \mid x \right) := \frac{q}{q-1} \sum_{\chi} \left(\frac{A_0\chi}{\chi} \right) \left(\frac{A_1\chi}{B_1\chi} \right) \cdots \left(\frac{A_n\chi}{B_n\chi} \right) \chi(x),$$

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

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

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

\begin{align*}
(a) \quad & p \cdot \binom{\phi}{\phi} | t \binom{\varepsilon}{t} = -\phi(-1)a_p(2E_1) \\
(b) \quad & p^2 \cdot \binom{\phi}{\phi} | 1 + \frac{1}{t} \binom{\varepsilon}{t} = \phi(-t)(a_p(3E_2)^2 - p),
\end{align*}

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 $\xi \in \mathbb{F}_p^\times$ 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

\[
p \cdot \binom{\xi}{\xi^5} | t \binom{\varepsilon}{t} = \frac{-\phi(2)}{\xi^3(1-t)}a_p(E_t).
\]

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

$$E_{a_1,a_3} : y^2 + a_1 xy + a_3 y = x^3$$

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 $\rho \in \hat{\mathbb{F}}_q^\times$ 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

$$a_q(\tilde{E}_{a_1,a_3}) = -q \cdot 2F_1\left(\frac{\rho}{\varepsilon}, \frac{\rho^2}{\varepsilon} \mid \frac{27a_3}{a_1^3}\right).$$

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 $T \in \hat{\mathbb{F}}_q^\times$ a generator of the character group. The trace of the Frobenius map on $E$ can be expressed as

$$a_q(E) = -q \cdot T^{\frac{q-1}{12}} \left(\frac{1728}{\Delta(E)}\right) \cdot 2F_1\left(\frac{T^{q-1}}{1728}, \frac{T^{q-1}}{\Delta(E)} \mid \frac{j(E)}{1728}\right),$$

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

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

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

\[
#C_z^{(a,b)}(\mathbb{F}_q) = q + 1 + q \sum_{i=1}^{\ell-1} \chi^{itb}(-1)_{2F1} \left( \chi^{it(1-a)}, \chi^{it(1-b)} \mid z \right),
\]

where \( \chi \in \hat{\mathbb{F}_q}^\times \) 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 \( 2F1 \) 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 \( 2F1 \) classical hypergeometric series as

\[
_{2} F_{1} \left( \begin{array}{c} a, b \cr c \end{array} \mid z \right) = \frac{(a)_n(b)_n}{(c)_n} \frac{z^n}{n!}.
\]
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

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

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

**Theorem 1.3.1.** [9, p. 115] For \( \text{Re} \, c > \text{Re} \, b > 0 \),

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

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]

\[ _2F_1 \left( \begin{array}{c} a, b \\ c \end{array} \middle| x \right) = (1 - x)^{-a} _2F_1 \left( \begin{array}{c} a, c - b \\ c \end{array} \middle| \frac{x}{x - 1} \right). \]

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 \( \text{Re} \, (c - a - b) > 0 \), then

\[ _2F_1 \left( \begin{array}{c} a, b \\ c \end{array} \middle| 1 \right) = \frac{\Gamma(c)\Gamma(c - a - b)}{\Gamma(c - a)\Gamma(c - b)}. \]

Further, the Kummer’s Theorem is given by

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

\[ _2F_1 \left( \begin{array}{c} a, b \\ 1 + b - a \end{array} \middle| -1 \right) = \frac{\Gamma(1 + b - a)\Gamma(1 + \frac{b}{2})}{\Gamma(1 + b)\Gamma(1 + \frac{b}{2} - a)}. \]
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 $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ is a cyclic multiplicative group of order $q - 1$. A multiplicative character $\chi : \mathbb{F}_q^* \to \mathbb{C}^*$ is a group homomorphism. Throughout, we reserve the notations $\varepsilon$ and $\phi$ for trivial and quadratic characters, respectively. Thus, for $x \in \mathbb{F}_q^*$

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

and

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

is the Lagrange 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 $j = 0, 1, 2, \ldots, q - 2$, the function

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

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

The set $\hat{\mathbb{F}}_q^*$ of all multiplicative characters on $\mathbb{F}_q^*$ is a cyclic group under multiplication of characters [6, 23, 29]. One extends the domain of all multiplicative characters $\chi$ on $\mathbb{F}_q^*$ 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 $a \in \mathbb{F}_p^*$. 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 $\hat{\mathbb{F}}_q^\times$. 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 $A \in \hat{\mathbb{F}}_q^\times$, 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 $\hat{\mathbb{F}}_q^\times$, 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
\[
G_m G_{-n} = q \left( \frac{T^m}{T^n} \right) G_{m-n} T^n (-1) = J(T^m, T^{-n}) G_{m-n}.
\]

### 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 \( \left( \begin{array}{c} A \\ B \end{array} \right) \) is defined by
\[
\left( \begin{array}{c} A \\ B \end{array} \right) := \frac{B(-1)}{q} J(A, B) = \frac{B(-1)}{q} \sum_{x \in \mathbb{F}_q} A(x) B(1-x),
\]

where \( B \) 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]
\[
\left( \begin{array}{c} A \\ \varepsilon \end{array} \right) = \left( \begin{array}{c} A \\ A \end{array} \right) = -\frac{1}{q} + \frac{q-1}{q} \delta(A),
\]
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 $A_0, A_1, \ldots, A_n$ and $B_1, B_2, \ldots, B_n$ in $\hat{\mathbb{F}}_q$, the Gaussian hypergeometric series $n+1F_n$ is defined to be

$$n+1F_n \left( \begin{array}{c} A_0, A_1, \ldots, A_n \\ B_1, \ldots, B_n \end{array} \bigg| x \right) : = \frac{q}{q-1} \sum_{\chi \in \hat{\mathbb{F}}_q} (A_0 \chi)(A_1 \chi) \cdots (A_n \chi) (B_1 \chi) \cdots (B_n \chi) \chi(x).$$

Greene also provided an alternative definition of $2F_1$ Gaussian hypergeometric function as follows.

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

$$2F_1 \left( \begin{array}{c} A, B \\ C \end{array} \bigg| x \right) = \varepsilon(x) \frac{BC(-1)}{q} \sum_{y \in \mathbb{F}_q} B(y)BC(1-y)A(1-xy). \quad (1.3.3)$$

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 $A_1, \ldots, A_n$ and $B_1, \ldots, B_n$ on $\mathbb{F}_q$, let

$$\left( \begin{array}{c} \vec{A} \\ \vec{B} \end{array} \right)$$

denotes the product

$$\prod_{k=1}^{n} \left( \frac{A_k}{B_k} \right).$$

Further, let

$$F \left( \begin{array}{c} C, \vec{A} \\ \vec{B} \end{array} \bigg| x \right)$$

denotes the series

$$n+1F_n \left( \begin{array}{c} C, A_1, \ldots, A_n \\ B_1, \ldots, B_n \end{array} \bigg| x \right).$$

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 $x \in \mathbb{F}_q$

$$F \left( \begin{array}{c} A, B, C, \vec{D} \\ E, B, \vec{F} \end{array} \bigg| x \right) = \frac{(CE)}{(BE)} F \left( \begin{array}{c} A, C, \vec{D} \\ E, \vec{F} \end{array} \bigg| x \right) - \frac{BE(-1)}{q} B(x) \left( \frac{AB}{B} \right) \times \left( \frac{\vec{D}B}{\vec{F}B} \right) + \frac{q-1}{q^2} BE(-1) F \left( \begin{array}{c} A, \vec{D} \\ \vec{B} \end{array} \bigg| x \right) \delta(CE).$$
Theorem 1.3.14. [18, Thm. 4.2 (ii)] For characters $A, B, D, \longrightarrow C, \longrightarrow E$ of $\mathbb{F}_q$ and $x \in \mathbb{F}_q$,

$$F \left( \begin{array}{c} A, B, \longrightarrow C, \longrightarrow D, \longrightarrow E | x \end{array} \right) = \frac{A \longrightarrow D \longrightarrow C \longrightarrow E (1) A(x) F \left( \begin{array}{c} A, A \longrightarrow D, A \longrightarrow E | \frac{1}{x} \end{array} \right)}{A \longrightarrow B, A \longrightarrow C | 1 - x}.$$

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 $x \in \mathbb{F}_q$,

(i) $2F_1 \left( \begin{array}{c} A, B, \longrightarrow C, \longrightarrow D, \longrightarrow E | x \end{array} \right) = A(-1) 2F_1 \left( \begin{array}{c} A, B \longrightarrow C, \longrightarrow D, \longrightarrow E | 1 - x \end{array} \right)$

$$+ A(-1) \left( \begin{array}{c} B \longrightarrow C, \longrightarrow D, \longrightarrow E | 1 - x \end{array} \right) \delta(1 - x) - \left( \begin{array}{c} B \longrightarrow C, \longrightarrow D, \longrightarrow E | x \end{array} \right) \delta(x),$$

(ii) $2F_1 \left( \begin{array}{c} A, B, \longrightarrow C, \longrightarrow D, \longrightarrow E | x \end{array} \right) = C(-1) A \longrightarrow C, \longrightarrow D, \longrightarrow E (1 - x) 2F_1 \left( \begin{array}{c} A, C \longrightarrow B, \longrightarrow C, \longrightarrow D, \longrightarrow E | x - 1 \end{array} \right)$

$$+ A(-1) \left( \begin{array}{c} B \longrightarrow C, \longrightarrow D, \longrightarrow E | 1 - x \end{array} \right) \delta(1 - x).$$

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

$$2F_1 \left( \begin{array}{c} A, \epsilon \longrightarrow B, \longrightarrow D, \longrightarrow E | x \end{array} \right) = \left( \begin{array}{c} B \longrightarrow A \longrightarrow D, \longrightarrow E | x \end{array} \right) A(-1) B(x) \longrightarrow A, \longrightarrow B (1 - x)$$

$$- \frac{1}{q} B(-1) \epsilon(x) + \frac{q - 1}{q} A(-1) \delta(1 - x) \delta(\longrightarrow A, \longrightarrow B).$$

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 $\theta(\alpha) = \zeta^{tr(\alpha)}$, where $\zeta = e^{\frac{2\pi i}{p}}$. For multiplicative characters $\chi, \psi \in \mathbb{F}_q^\times$, we have

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