TAIWANESE JOURNAL OF MATHEMATICS
Vol. 21, No. 1, pp. 55–79, February 2017
DOI: 10.11650/tjm.21.2017.7724
This paper is available online at http://journal.tms.org.tw

Rational Points over Finite Fields on a Family of Higher Genus Curves and Hypergeometric Functions

Yih Sung

Abstract. In this paper we investigate the relation between the number of rational points over a finite field $\mathbb{F}_{p^n}$ on a family of higher genus curves and their periods in terms of hypergeometric functions. For the case $y^\ell = x(x-1)(x-\lambda)$ we find a closed form in terms of hypergeometric functions associated with the periods of the curve. For the general situation $y^\ell = x^{a_1}(x-1)^{a_2}(x-\lambda)^{a_3}$ we show that the number of rational points is a linear combination of hypergeometric series, and we provide an algorithm to determine the coefficients involved.

1. Introduction

1.1. Background

The Legendre family of elliptic curves is defined explicitly by

$$X_\lambda = \left\{y^2 = x(x-1)(x-\lambda)\right\}$$

on $\mathbb{C}^2$, where $\lambda \in \mathbb{C} - \{0,1\} = P^1_{\mathbb{C}} - \{0,1,\infty\}$. It is generally understood that the number of rational points of X_λ over a finite field $\mathbb{F}_p$ with the prime p is related to a period integral on X_λ, which in turn is related to the Gauss hypergeometric series ${}_2F_1(\frac{1}{2},\frac{1}{2},1;\lambda)$ modulo p. This hypergeometric series is a solution of a hypergeometric differential equation in which the derivatives are given by the Gauss-Manin connection of the family. The first goal of this paper is to understand corresponding situations for more general families of Riemann surfaces $\{X_\lambda\}$ of higher genus. We want to give an explicit formula of the number of rational points on X_λ over a finite field $\mathbb{F}_p$ with the prime p in terms of period integrals or hypergeometric series, as in the case of the Legendre family. We are particularly interested in families associated with triangle groups, in which the Legendre family is a special case. It is important to note that a fibre curve X_λ in this family may have singularities, which makes the situation more complicated and interesting. We also investigate $\mathbb{F}_{p^n}$ because

Received June 22, 2016; Accepted August 16, 2016.
Communicated by Sai-Kee Yeung.
2010 *Mathematics Subject Classification.* 14G05, 30F30, 33C05.
Key words and phrases. Riemann surfaces, Rational points, Holomorphic differentials, Hypergeometric functions.

the case of $n > 1$ is more subtle than the case of $n = 1$. We will finally consider the counts modulo p and modulo p^n. The former situation is explained completely in this paper. For the latter situation, we will provide examples to demonstrate that the problem at hand is more subtle so that the general problem remains open.

The classical correspondence between the period of X_λ and the number of rational points on X_λ over $\mathbb{F}_p$ can be proved through brute force, as shown in [1]. By direct calculation, the number of rational points on X_λ is

$$\begin{aligned} |X_\lambda| &\equiv -(-1)^{(p-1)/2} \sum_{r=0}^{(p-1)/2} \binom{-1/2}{r}^2 \lambda^r \mod p \\ &= -(-1)^{(p-1)/2} {}_2F_{1,(p-1)/2}(\tfrac{1-p}{2}, \tfrac{1-p}{2}, 1; \lambda) \mod p. \end{aligned} \tag{1.1}$$

To clarify the subindex of F, $(p-1)/2$ refers to the truncation in the summation. Note that the Gauss hypergeometric function ${}_2F_1(a, b, c; \lambda)$ satisfies a second-order differential equation

$$x(x-1)\frac{\mathrm{d}^2 u}{\mathrm{d}x^2} + ((a+b+1)x - c)\frac{\mathrm{d}u}{\mathrm{d}x} + ab \cdot u = 0. \tag{1.2}$$

It is surprising that the number of rational points on X_λ is related to a solution of a differential equation defined on the base of the family. In papers [3] and [4] Manin explained this phenomenon by applying the Lefschetz Fixed Point Formula. Since $h^0(X_\lambda, K) = 1$ the holomorphic differential $\omega_\lambda = \mathrm{d}x/y$ generates $H^0(X_\lambda, K)$. Manin observed that by taking the local coordinate x of X_λ and fixing a base point $\mathfrak{q}$, ω_λ can be expressed as

$$\omega_\lambda = \mathrm{d}x + \sum_{r \geq 1} a_r (x - x(\mathfrak{q}))^r \mathrm{d}x.$$

Then by the Lefschetz fixed-point theorem Manin showed that a_{p-1} satisfies the Picard-Fuch equation (1.2) modulo p. Therefore periods of X_λ are related to the number of rational points on X_λ modulo $\mathbb{F}_p$ and satisfy the hypergeometric equation (1.2).

1.2. Statement of results

We consider the family of curves defined by $y^\ell = x(x-1)(x-\lambda)$ and $y^\ell = x^{a_1}(x-1)^{a_2}(x-\lambda)^{a_3}$ with assumptions that $a_1, a_2, a_3 \in \mathbb{Z}_{>0}$, $(\ell, a_1, a_2, a_3) = 1$ and $\alpha = a_1 + a_2 + a_3 \leq \ell$. For the first family, we offer a formula in a closed form:

Theorem 1.1. *Let $m \geq 4$, ℓ be integers. Let X_λ^m be the family of algebraic curves defined by $y^m = x(x-1)(x-\lambda)$ over the finite field $\mathbb{F}_q$, $q = p^n$, with the parameter $\lambda \in \mathbb{Q}$. Let $\ell = (m, q-1)$, so that ℓ satisfies $\ell \mid (q-1)$. If $\ell = 1$, the number of rational points on X_λ is*

$$\left|X_{\lambda,p}^m\right| \equiv 0 \mod p.$$

If $\ell \geq 2$, let S_{reg} and S_{irr} be sets such that

$$S_{\mathrm{reg}} = \left\{ (0,s),(1,s') \;\middle|\; \frac{\ell}{2} - 1 \leq s \leq \ell - \left[\frac{\ell}{3}\right] - 2,\ 0 \leq s' \leq \ell - \left[\frac{2\ell}{3}\right] - 2 \right\},$$

$$S_{\mathrm{irr}} = \left\{ (0,s) \;\middle|\; 0 \leq s < \frac{\ell}{2} - 1 \right\},$$

and denote $a = 2 - \frac{3(s+1)}{\ell} - r$, $b = 1 - \frac{(s+1)}{\ell}$, $c = 2\left(1 - \frac{(s+1)}{\ell}\right) - r = 2b - r$. Then

$$\begin{aligned} \left|X^m_{\lambda,q}\right| \equiv & \sum_{(r,s)\in S_{\mathrm{reg}}} -k_{r,s} \cdot {}_2F_{1,N_{r,s}}(a,b,c;\lambda) \\ & + \sum_{(r,s)\in S_{\mathrm{irr}}} -k'_{r,s} \cdot \lambda^{M_{r,s}} {}_2F_{1,N'_{r,s}}(a-c+1, b-c+1, -c+2; \lambda) - \delta \mod p, \end{aligned}$$

where $\delta = (\ell, 3) - 1$,

$$N_{r,s} = \left(2 - r - \frac{3(s+1)}{\ell}\right)(q-1), \quad k_{r,s} = (-1)^{N_{r,s}} \binom{\frac{(\ell-s-1)(q-1)}{\ell}}{N_{r,s}}$$

and

$$M_{r,s} = \left(1 - \frac{2(s+1)}{\ell}\right)(q-1), \quad N'_{r,s} = \frac{s+1}{\ell}(q-1), \quad k'_{r,s} = (-1)^{N_{r,s}} \binom{\frac{(\ell-s-1)(q-1)}{\ell}}{M_{r,s}}.$$

In a more general case, we derive the following result.

Theorem 1.2. *Let $m \geq 4$, ℓ be integers, and Y^ℓ_λ be the family of algebraic curves defined by $y^\ell = x^{a_1}(x-1)^{a_2}(x-\lambda)^{a_3}$ over the finite field $\mathbb{F}_q$ where $q = p^n$. Assume $\ell, a_1, a_2, a_3 \in \mathbb{Z}_{>0}$, $(\ell, a_1, a_2, a_3) = 1$, $\alpha = a_1 + a_2 + a_3 \leq \ell$, and $\ell \mid (q-1)$. Then*

$$|Y_{\lambda,q}| \equiv \sum_{k=1}^{\ell} \left(\sum_{\alpha\in B} -c_\alpha F_{N_\alpha}(a_\alpha, b_\alpha, c_\alpha; \lambda) - \sum_m \delta_{k,m}\lambda^m \right) \pmod p,$$

where B is a basis of holomorphic one forms on Y^ℓ_λ and $F_{N_\alpha}(a_\alpha, b_\alpha, c_\alpha; \lambda)$ are the associated hypergeometric functions for some $a_\alpha, b_\alpha, c_\alpha \in \mathbb{Q}$, and $\delta_{k,m}$ are rational numbers reflecting the singularities of the curves.

An explicit algorithm to find the constants involved in the above theorem is presented in the appendix.

We note that to combine the classical counting technique and the Lefschetz fixed-point theorem is necessary. If we apply only classical counting methods, it is difficult to see how counting is related to the periods of holomorphic differentials; on the other hand, if we apply only the Lefschetz fixed-point theorem we cannot determine precise constants for each hypergeometric function.

Compared to the Legendre family of elliptic curves, there are a few significant differences that we need to address. First, the algebraic curves we are interested have singularities. Therefore, we need to apply normalization or to use a desingularisation model of the curves in order to apply the Lefschetz Fixed Point Formula. The difference in counting on the number of rational points in the affine part of the normalization and the curve itself gives rise to an expression that we call the *correction term* in this article, represented by δ and $\delta_{k,m}$ in the above theorems. Secondly, there are more than one choice of basis of the space of holomorphic differentials. Thus, we need to consider an appropriate linear combination of period integrals or appropriate hypergeometric functions in order to compute the explicit coefficients in Theorem 1.2. Finally, we consider the finite field $\mathbb{F}_q$ where $q = p^n$ and $n > 1$. For most of our results, we consider the number of rational points in $\mathbb{F}_{p^n}$ modulo p. The situation of rational points in $\mathbb{F}_{p^n}$ modulo p^n will be explained by explicit examples in the last section.

1.3. Contents

Throughout this article, we assume that $\lambda \in \mathbb{C} - \{0, 1\}$. We derive the closed formula for the case $y^\ell = x(x-1)(x-\lambda)$ in Section 2. In Section 3, we give an algorithm to handle the case $y^\ell = x^{a_1}(x-1)^{a_2}(x-\lambda)^{a_3}$. In Section 4, we remark on an extension of results from the finite field $\mathbb{F}_p$ to $\mathbb{F}_{p^n}$ for elliptic curves and make some observations about the truncation levels of the hypergeometric functions involved. In the last section, we list several examples to illustrate subtle points in the formulations and computations of our theorems.

2. Case of X defined by $y^\ell = x(x-1)(x-\lambda)$

2.1. Genus formula and Abelian differentials

Let us consider a family of curves X_λ defined by

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

over the finite field $\mathbb{F}_q$ where $q = p^n$. Let C_λ be a smooth model of the projectivization of X_λ. Let $X_{\lambda,q}$ be the curve defined over $\mathbb{F}_q$. For brevity, we drop the dependence on λ and q and simply denote a curve in the family by X. By the defining equation, we know $H^0(X, K_X)$ is generated by the Abelian differentials

$$\omega_{r,s} = x^r y^s \frac{\mathrm{d}x}{y^{\ell-1}} = x^r [x(x-1)(x-\lambda)]^{[s-(\ell-1)]/\ell}\,\mathrm{d}x \tag{2.1}$$

and we will find the appropriate range of r and s later. For $\ell \leq 4$, by checking the smoothness at ∞ after change of coordinates we may simply apply the genus formula. For

$\ell > 4$, after compactification in $\mathbb{P}^2$, the curve is defined by

$$W_1^\ell = W_0(W_0 - W_2)(W_0 - \lambda W_2)W_2^{\ell-3}.$$

Specialize to the affine open set $U_{W_0=1}$, and the curve is defined by $y^\ell = (1-z)(1-\lambda z)z^{\ell-3}$ which has a singularity at $(0,0)$. Let C be a smooth model of X. To find the genus of C, the standard method is to apply the Hurwitz Formula.

Lemma 2.1. [2, Theorem 3] *Let $\ell > 4$.*

(a) *The genus of C is given by*

$$g(C) = \begin{cases} \ell - 2 & \text{if } 3 \mid \ell, \\ \ell - 1 & \text{if } 3 \nmid \ell. \end{cases}$$

(b) *Denoted by $[a]$ the integral part of a. A basis of holomorphic one forms on C is given by $\frac{\mathrm{d}x}{y^i}$ and $\frac{x\,\mathrm{d}x}{y^j}$, where $[\frac{\ell}{3}] + 1 \le i \le \ell - 1$ and $[\frac{2\ell}{3}] + 1 \le j \le \ell - 1$.*

After resolving the singularities of X, we get a smooth model C in

$$\mathbb{P}^2 \times \mathbb{P}^1 \times \cdots \times \mathbb{P}^1.$$

The coordinates are $(x, y, z; z_1, t_1; y_1, w_1; \ldots; y_i, w_i; \ldots)$ and C is defined by $y^\ell = x(x-1)(x-\lambda)$ and the associated equations of blowup. Once x and y are determined, the rest of the values are determined accordingly. Thus, away from the singularities and their preimage on the blowup there is a one-one correspondence of rational points between X and C. This implies that we can count the number of rational points on C. Since the Lefschetz Fixed Point Formula requires that the curve is smooth, we must consider the smooth model C rather than X. Then we consider the Frobenius map

$$F_b(x, y, z; z_1, t_1; y_1, w_1; \ldots; y_i, w_i; \ldots) = (x^q, y^q, z^q; z_1^q, t_1^q; y_1^q, w_1^q; \ldots; y_i^q, w_i^q; \ldots),$$

and the classical argument applies. For the computation of the trace map, we localize the computation to an affine open set U of C by choosing $U = C - \infty = X - \infty$. Then we take the local parameter x to continue on the computation.

2.2. Hypergeometric functions and periods

By Lemma 2.1, we know that the basis of holomorphic 1-forms can be chosen as

$$\omega_{0,s},\ 0 \le s \le \ell - \left[\frac{\ell}{3}\right] - 2, \quad \text{and} \quad \omega_{1,s},\ 0 \le s \le \ell - \left[\frac{2\ell}{3}\right] - 2. \tag{2.2}$$

Recalling the formula of the period

$$ {}_2F_1(a,b,c;x) = \frac{\Gamma(c)}{\Gamma(b)\Gamma(c-b)} \int_0^1 t^{b-1}(1-t)^{c-b-1}(1-xt)^{-a}\,\mathrm{d}t, $$

and comparing $\omega_{r,s}$ with the differential in the integral, we have

$$ a = \frac{\ell - s - 1}{\ell}, \quad b = r + \frac{s+1}{\ell}, \quad c = r + \frac{2(s+1)}{\ell}. \tag{2.3} $$

Hence a change of coordinate $\lambda = 1/x$ is needed. We have an technical observation:

Proposition 2.2. *Letting $\lambda = 1/x$, the analytic continuation of $x^a \cdot {}_2F_1(a,b,c;x)$ at ∞ is ${}_2F_1(a-c+1, a, a-b+1; \lambda)$.*

Proof. The change of variable $x = 1/\lambda$ means that we study the behavior of the hypergeometric series at ∞ after analytic continuation. Note that ∞ here *does not* mean the ∞ of X. It simply means the change of variable $x = 1/\lambda$. By taking an appropriate branch cut in the domain to take roots of -1 we can consider the period integral

$$ \lambda^{-a}\,{}_2F_1(a,b,c;1/\lambda) = \frac{\Gamma(c)(-1)^{-a-b+c-1}}{\Gamma(b)\Gamma(c-b)} \int_0^1 t^{b-1}(t-1)^{c-b-1}(t-\lambda)^{-a}\,\mathrm{d}t \tag{2.4} $$

with $c > b > 0$. Multiplying λ^α to (1.2) we have

$$ (\lambda-1)\lambda^{\alpha+2}\frac{\mathrm{d}^2u}{\mathrm{d}\lambda^2} + ((2-c)\lambda + (a+b-1))\lambda^{\alpha+1}\frac{\mathrm{d}u}{\mathrm{d}\lambda} - ab\lambda^\alpha u = 0. \tag{2.5} $$

Our plan is to replace u with $\lambda^\alpha u$ and find an appropriate α such that $u\lambda^\alpha$ satisfies a new hypergeometric differential equation. By direct calculation, the above equation can be rewritten as

$$ \lambda(\lambda-1)\frac{\mathrm{d}^2}{\mathrm{d}\lambda^2}(\lambda^\alpha u) + [(2-c+2a)\lambda + (-a+b-1)]\frac{\mathrm{d}}{\mathrm{d}\lambda}(\lambda^\alpha u) + a(a-c+1)(\lambda^\alpha u) = 0 $$

by taking $\alpha = -a$ and dividing two sides by λ. Comparing with (1.2) we have

$$ \begin{cases} a' + b' + 1 = 2a - c + 2, \\ -c' = -a + b - 1, \\ a' \cdot b' = a(a-c+1), \end{cases} \quad \Longrightarrow \quad \begin{cases} a' = a - c + 1, \\ b' = a, \\ c' = a - b + 1. \end{cases} $$

Hence the proof is complete. □

Let us end the subsection by introducing a notation.

Notation 2.3. The truncated hypergeometric series is defined by

$$ {}_2F_{1,N}(a,b,c;\lambda) := \sum_{k=0}^{N} \frac{(a)_k (b)_k}{(c)_k\, k!}\lambda^k. $$

Similarly, we denote $F_N(a,b,c;x)$ the truncated hypergeometric series of $F(a,b,c;x)$, which is a solution to the hypergeometric equation (1.2).

2.3. Counting rational points

Let us consider the Frobenius map $F_b(x) = x^q$ on the normalization C_λ of X_λ. Applying the Lefschetz fixed-point theorem to F_b, we have [1, (2.34)]

$$1 - \mathrm{Tr}(F_b^*|_{H^1(C_\lambda,\mathcal{O})}) = \text{number of fixed points of } F_b.$$

Recall that the number of rational points on X_λ is denoted by $|X_\lambda|$. Therefore, we get

$$\begin{aligned} |X_\lambda| &= -\mathrm{Tr}(F_b^*|_{H^1(C_\lambda,\mathcal{O})}) - (|\text{points at } \infty \text{ on } C_\lambda| - 1) \\ &\equiv \sum_{(r,s)\in S} -k_{r,s} \cdot F_{N_{r,s}}(2 - r - \tfrac{3(s+1)}{\ell}, \tfrac{\ell-s-1}{\ell}, 2 - r - \tfrac{2(s+1)}{\ell}; \lambda) - \delta_\infty \mod p \end{aligned} \tag{2.6}$$

for some constants $k_{r,s}$ $N_{r,s}$, δ_∞, where S is the set of subscripts defined in (2.2), and $\delta_\infty = |\text{points at } \infty \text{ on } C_\lambda| - 1$. Note that in the second congruence identity, We take $\{\omega_{r,s}\}_{(r,s)\in S}$ as the basis of $H^1(C_\lambda, \mathcal{O})$, applying the similar technique in the calculation of the classical case of elliptic curves, and then each element $\omega_{r,s}$ in the basis will contribute $k_{r,s} \cdot F_{N_{r,s}}(a', b', c'; \lambda)$ to the trace of F_b^*. The parameters of the hypergeometric functions $a' = 2 - r - \frac{3(s+1)}{\ell}$, $b' = 1 - \frac{s+1}{\ell} = \frac{\ell-s-1}{\ell}$, $c' = 2 - r - \frac{2(s+1)}{\ell}$ are determined by (2.3) and Proposition 2.2. In addition, the term δ_∞ in (2.6) denotes the difference between the number of rational points at ∞ on C_λ and X_λ, and we call δ_∞ the *correction term* at ∞. Our goal is to determine these constants by counting rational points over some primes.

First, let us explain how to compute δ_∞. In Lemma 2.1 we saw if $(3, \ell) = 3$, the point at infinity of the smooth model C_λ splits into three points, and if $(3, \ell) = 1$ the smooth model has only one point at infinity of C_λ. On the other hand $|X_\lambda^m|$ only counts the rational points in $U_{W_2=1}$, so for the case $(3, \ell) = 3$ we have to make a correction $-(3-1)$. These corresponds to $\delta_\infty = 0$ or 2 respectively.

Consider q such that

$$\ell \mid (q-1). \tag{2.7}$$

This implies $(\ell, p) = 1$ and $\ell \not\equiv 0 \mod p$, so the fractions in (2.6) are well defined. In the following counting process, we need a criterion of the existence of ℓ-roots:

Lemma 2.4. *Let $\ell \mid (q-1)$ and $a \in \mathbb{F}_q$. Then*

$$a^{(q-1)/\ell} \equiv \begin{cases} 1 & \text{iff } a = y^\ell \text{ for some } y, \\ \text{other values} & \text{there does not exist } y \text{ such that } a = y^\ell. \end{cases} \tag{2.8}$$

Proof. The proof follows the lines of the proof of the classical case, namely the case of $\ell = 2$. If there exists y such that $a = y^\ell$, then

$$a^{(q-1)/\ell} \equiv y^{q-1} \equiv 1 \quad \text{in } \mathbb{F}_q$$

by the little Fermat theorem. Conversely, we assume $a^{(q-1)/\ell} \equiv 1$. Consider the algebraic closure Ω of $\mathbb{F}_q$ such that Ω contains all roots of the algebraic equations $y^\ell \equiv b$ for $b \in \mathbb{F}_q$. Thus $a = y^\ell$ is solvable in Ω. Then the assumption $a^{(q-1)/\ell} \equiv 1$ implies $y^{q-1} \equiv 1$ in Ω. However, the equation $y^{q-1} - 1 \equiv 0$ is solvable in $\mathbb{F}_q$. Let $\mathbb{F}_q^* = \langle \alpha \rangle$, then

$$y^{q-1} - 1 \equiv (y - \alpha)(y - \alpha^2) \cdots (y - \alpha^{q-1}).$$

Therefore, $y \in \mathbb{F}_q$. □

Now we want to count the number of rational points on $X_{\lambda,q}$. Given a pair $(x, y) \in X_{\lambda,q}$ we apply (2.8) to $x(x-1)(x-\lambda)$ to see if (x, y) is a rational point on $X_{\lambda,q}$. Let $t = [x(x-1)(x-\lambda)]^{(q-1)/\ell}$. We intend to find a polynomial $f(t)$ satisfying

$$f(0) = 1,\ f(1) = \ell,\ f(\zeta^i) = 0 \quad \text{for } 0 \le i \le \ell - 1.$$

This means that if $x(x-1)(x-\lambda) = 0$, there is only one point $(x, 0)$ on $X_{\lambda,q}$; if $x(x-1)(x-\lambda)^{1/\ell}$ exists in $\mathbb{F}_q$, there are ℓ points on $X_{\lambda,q}$; if $x(x-1)(x-\lambda)^{1/\ell}$ does not exist in $\mathbb{F}_q$, (x, y) is not a rational point on $X_{\lambda,q}$. Observe that the simplest function f satisfying $f(\zeta^i) = 0$ for $0 \le i \le \ell - 1$ is

$$f(t) = (t - \zeta)(t - \zeta^2) \cdots (t - \zeta^{\ell-1}) = \frac{t^\ell - 1}{t - 1} = 1 + t + \cdots + t^{\ell-1},$$

and $f(t)$ also satisfies $f(0) = 1$ and $f(1) = \ell$. Hence f is a counting function and we have

$$|X_\lambda| \equiv \sum_{x \in \mathbb{F}_q} (t + \cdots + t^{\ell-1}) \mod p.$$

Let us compute each term $\sum_x t^k$. The highest power of x in $\sum_x t^k$ is $\frac{3k}{\ell}(q-1)$. By the observations

$$\sum_{x \in \mathbb{F}_q} x^k \equiv \begin{cases} -1 \mod p & \text{if } (q-1) \mid k, \\ 0 \mod p & \text{if } (q-1) \nmid k, \end{cases} \tag{2.9}$$

we need the power to be a multiple of $(q-1)$, which implies

$$3k \ge \ell.$$

By the range $0 \le k \le \ell - 1$, we know $\lceil \frac{\ell}{3} \rceil \le k \le \ell - 1$. For simplicity, let us first consider the case $\delta = 0$ and we will come back to the case $\delta \ne 0$ later. Assume that $\delta = 0$

or $(3,\ell)=1$ and recall that $\ell \mid (q-1)$. By the power series expansion, we get

$$\begin{aligned}\sum_{x\in\mathbb{F}_q} t^k &= \sum_{x\in\mathbb{F}_q} x^{\frac{k(q-1)}{\ell}} \sum_m \binom{\frac{k(q-1)}{\ell}}{m}(-1)^m x^{\frac{k(q-1)}{\ell}-m} \sum_n \binom{\frac{k(q-1)}{\ell}}{n}(-\lambda)^n x^{\frac{k(q-1)}{\ell}-n} \\ &= \sum_{x\in\mathbb{F}_q} x^{\frac{k(q-1)}{\ell}} \sum_{m,n} \binom{\frac{k(q-1)}{\ell}}{m}\binom{\frac{k(q-1)}{\ell}}{n}(-1)^{m+n}\lambda^n \cdot x^{\frac{2k(q-1)}{\ell}-(m+n)} \qquad (2.10)\\ &= \sum_{x\in\mathbb{F}_q}\sum_N (-1)^N \sum_{m+n=N} \binom{\frac{k(q-1)}{\ell}}{m}\binom{\frac{k(q-1)}{\ell}}{n}\lambda^n \cdot x^{\frac{2k(q-1)}{\ell}-(m+n)} x^{\frac{k(q-1)}{\ell}}.\end{aligned}$$

Definition 2.5. For fixed k the counting in (2.10) is called a weight-k counting of $|X_{\lambda,q}|$.

Let us examine the numerical conditions closely. m, n in (2.10) come from the binomial expansion, so they are required to be integers. Plus (2.9) we can write $N = \left(\frac{3k}{\ell} - r - 1\right)(q-1)$ for some $r \in \mathbb{Z}_{\geq 0}$ satisfying

$$\begin{aligned}\frac{k(q-1)}{\ell} \geq N &\implies \left(r+1-\frac{2k}{\ell}\right)(q-1) \geq 0 \\ &\implies \left(r+1-\frac{2k}{\ell}\right) \geq 0. \qquad (2.11)\end{aligned}$$

If $r=1$ (2.11) always holds, because $k \leq \ell - 1 < \ell$. If $r=0$ (2.11) becomes

$$1 - \frac{2k}{\ell} \geq 0 \implies \frac{\ell}{2} \geq k.$$

Thus, we divide the situation into two cases.

- *Regular parameters.* $r=1$, $\left\lceil \frac{\ell}{3} \right\rceil \leq k \leq \ell - 1$; and $r=0$, $\left\lceil \frac{\ell}{3} \right\rceil \leq k \leq \frac{\ell}{2}$.
- *Irregular parameters.* $r=0$, $\frac{\ell}{2} < k \leq \ell - 1$.

2.4. Contributions from regular parameters

By (2.9) we observe that the non-zero terms in (2.10) corresponding to the power of x satisfy

$$\frac{2k(q-1)}{\ell} - (m+n) + \frac{k(q-1)}{\ell} = (r+1)(q-1)$$

for some $r \in \mathbb{Z}_{\geq 0}$. Hence

$$N = m + n = \left(\frac{3k-\ell}{\ell} - r\right)(q-1) \qquad (2.12)$$

for some $r \in \mathbb{Z}_{\geq 0}$, and the coefficients are

$$\begin{aligned}&-(-1)^N \sum_{n=0}^{N} \binom{\frac{k(q-1)}{\ell}}{N-n}\binom{\frac{k(q-1)}{\ell}}{n}\lambda^n \qquad (2.13)\\ &\equiv -(-1)^N \binom{\frac{k(q-1)}{\ell}}{N} \cdot {}_2F_{1,N}\left(\tfrac{3k}{\ell} - r - 1, \tfrac{k}{\ell}, \tfrac{2k}{\ell} - r; \lambda\right) \mod p.\end{aligned}$$

Compare (2.13) with (2.6) and we have

$$k = \ell - s - 1. \tag{2.14}$$

Therefore,

$$N_{r,s} = \left(2 - r - \frac{3(s+1)}{\ell}\right)(q-1),$$
$$k_{r,s} = (-1)^{N_{r,s}} \binom{\frac{(\ell-s-1)(q-1)}{\ell}}{N_{r,s}}.$$

By construction, $N_{r,s} \in \mathbb{Z}_{>0}$. This implies

$$2 - r - \frac{3(s+1)}{\ell} > 0 \implies r = 0, 1. \tag{2.15}$$

For $r = 0$, the inequality becomes

$$\begin{aligned} \frac{2\ell}{3} - 1 > s &\implies 2k + \frac{2\gamma}{3} - 1 > s, && \text{(by writing } \ell = 3k + \gamma) \\ &\implies (2k + \gamma - 1) - \frac{\gamma}{3} > s, \end{aligned}$$

which matches (2.2), because in (2.2) the equation reads

$$\begin{aligned} s \leq \ell - \left[\frac{\ell}{3}\right] - 2 &\implies s \leq (3k + \gamma) - k - 2 \\ &\implies s \leq (2k + \gamma - 1) - 1 < (2k + \gamma - 1) - \frac{\gamma}{3}. \end{aligned}$$

For $r = 1$, (2.15) becomes

$$\frac{\ell}{3} - 1 > s \implies k + \frac{\gamma}{3} - 1 > s \implies (k + \gamma - 1) - \frac{2\gamma}{3} > s,$$

which also matches (2.2), because in (2.2) the equation reads

$$\begin{aligned} s \leq \ell - \left[\frac{2\ell}{3}\right] - 2 &\implies s \leq (3k + \gamma) - \left(2k + \left[\frac{2\gamma}{3}\right]\right) - 2 \\ &\implies s \leq (k + \gamma - 1) - \left(\left[\frac{2\gamma}{3}\right] + 1\right) < (k + \gamma - 1) - \frac{2\gamma}{3}. \end{aligned}$$

This concludes the computation of the regular parameters.

2.5. Contributions from irregular parameters

We redo the computation:

$$
\begin{aligned}
&-(-1)^N \sum_{n=0}^{N} \binom{\frac{k(q-1)}{\ell}}{N-n}\binom{\frac{k(q-1)}{\ell}}{n}\lambda^n \\
&= -(-1)^N \sum_{n=\left(\frac{2k}{\ell}-1\right)(q-1)}^{k(q-1)/\ell} \binom{\frac{k(q-1)}{\ell}}{N-n}\binom{\frac{k(q-1)}{\ell}}{n}\lambda^n \\
&= -(-1)^N \binom{\frac{k(q-1)}{\ell}}{\frac{(2k-\ell)(q-1)}{\ell}} \lambda^{\frac{(2k-\ell)(q-1)}{\ell}} \cdot {}_2F_1\left(\tfrac{(k-\ell)(q-1)}{\ell}, \tfrac{k}{\ell}(1-q), \tfrac{2k(q-1)-\ell(q-2)}{\ell}; \lambda\right) \\
&\equiv -(-1)^{\frac{(3k-\ell)}{\ell}(q-1)} \binom{\frac{k(q-1)}{\ell}}{\frac{(2k-\ell)(q-1)}{\ell}} \lambda^{\frac{(2k-\ell)(q-1)}{\ell}} {}_2F_1\left(\tfrac{\ell-k}{\ell}, \tfrac{k}{\ell}, \tfrac{2(\ell-k)}{\ell}; \lambda\right) \mod p.
\end{aligned}
\tag{2.16}
$$

Referring to (2.13), letting $a = \frac{3k-\ell}{\ell}$, $b = \frac{k}{\ell}$, $c = \frac{2k}{\ell}$ (because $r = 0$), one can recognize that the parameters in (2.16) are

$$(a - c + 1, b - c + 1, -c + 2).$$

Therefore, for the irregular parameters, F_N is chosen to be $x^{1-c}{}_2F_{1,N}(a - c + 1, b - c + 1, -c + 2; x)$. This can be justified in the partial summation because the lower bound $\frac{(2k-\ell)(q-1)}{\ell} > 0$.

In the above calculation, we assumed $\delta = 0$ or equivalently $(3, \ell) = 1$, so $N = m+n \neq 0$. Consider the case $(3, \ell) = 3 \Rightarrow \ell = 3\ell'$ and set $N = 0$ which implies

$$\frac{3k}{\ell} = \frac{k}{\ell'} = r + 1,$$

and we know $r = 0, 1$ which leads to $k = \ell'$, $2\ell' \leq 3\ell' - 1 = \ell - 1$. This means that there are two situations in which $N = 0$ and the summation $\sum[x(x-1)(x-\lambda)]^{k(q-1)/\ell}$ contains x^{q-1} or $x^{2(q-1)}$. Consequently, these two terms contribute -2 after summing over $\mathbb{F}_q$.

The above discussion, together with (2.13) and (2.16), concludes the proof of Theorem 1.1 in the case of $m = \ell$, with $\ell \mid (p - 1)$.

2.6. Conclusion of proof of Theorem 1.1

Lemma 2.6. *Let $d = (\ell, q-1) = \gcd(\ell, q-1)$ and S be the set of $\mathbb{F}_q^*$. Denote $S^n = \{a^n \mid a \in S\}$.*

(a) *If $\ell \nmid (q-1)$, then the number of rational points of $y^\ell = x(x-1)(x-\lambda)$ over $\mathbb{F}_q$ is the same as the number of rational points of $y^d = x(x-1)(x-\lambda)$ over $\mathbb{F}_q$.*

(b) *If $d = 1$, then $S^\ell = S$, namely for every $a \in \mathbb{F}_q$ the equation $y^\ell = a$ has a unique solution in $\mathbb{F}_q$.*

Proof. For (a), this is a basic property of the units $\mathbb{F}_p^*$ of a finite field $\mathbb{F}_p$. For (b), by the same property of $\mathbb{F}_q^*$, one can show $S^\ell = S$. □

By this lemma, we can always assume $\ell \mid (q-1)$ and if $d = (\ell, p-1) = 1$, the equation $y^\ell = x(x-1)(x-\lambda)$ has a unique solution in $\mathbb{F}_q$ for every $x \in \mathbb{F}_q$. Thus the counting polynomial is $f(t) = 1$ and we have

$$|X_{\lambda,q}| \equiv \sum_{x\in\mathbb{F}_q} 1 \equiv 0 \mod p.$$

Now we can complete the proof of Theorem 1.1 for general m as stated. Observe the following relation between $H^0(C_\lambda^m, K)$ and $H^0(C_\lambda^\ell, K)$, where C_λ^ℓ is the smooth model of the curve defined in $\mathbb{P}^2$ with the defining equation

$$W_1^\ell = W_0(W_0 - W_2)(W_0 - \lambda W_2)W_2^{\ell-3}.$$

In the affine piece $U_{W_2=1} \subset \mathbb{P}^2$, by (2.2) we want to show

$$m - \left[\frac{m}{3}\right] \geq \ell - \left[\frac{\ell}{3}\right] \quad \text{and} \quad m - \left[\frac{2m}{3}\right] \geq \ell - \left[\frac{2\ell}{3}\right]. \tag{2.17}$$

Write $m = \ell k$, and $\ell = 3q + r$, $0 \leq r \leq 2$. Then

$$m - \left[\frac{m}{3}\right] \geq \ell - \left[\frac{\ell}{3}\right] \quad \Longleftrightarrow \quad 2q(k-1) - r + \left(rk - \left[\frac{rk}{3}\right]\right)$$

since $2q(k-1) - r \geq 2[q(k-1) - 1] \geq 0$. For the other inequality,

$$m - \left[\frac{2m}{3}\right] \geq \ell - \left[\frac{2\ell}{3}\right] \quad \Longleftrightarrow \quad q(k-1) - \left(r - \left[\frac{2r}{3}\right]\right) + \left(rk - \left[\frac{2rk}{3}\right]\right) \geq 0$$

since $\left(r - \left[\frac{2r}{3}\right]\right) \leq 1$ (if $r = 2$, $\left[\frac{2r}{3}\right] = 1$; if $r = 1$, $\left[\frac{2r}{3}\right] = 0$). These two inequalities allow the local expression

$$x^{r+\frac{s-(\ell-1)}{\ell}}(x-1)^{\frac{s-(\ell-1)}{\ell}}(x-\lambda)^{\frac{s-(\ell-1)}{\ell}}\,\mathrm{d}x$$

of the differential $w_{r,s}$ to have the same format in $H^0(C^m, K)$ and $H^0(C^\ell, K)$, and allow the indices to match. Therefore, we can safely proceed the reduction and complete the proof.

3. Case of X defined by $y^\ell = x^{a_1}(x-1)^{a_2}(x-\lambda)^{a_3}$

3.1. Basic facts

We can apply the method developed in the preceding section to a more general situation. Let p be a prime and $q = p^n$. Let X_λ be the curve defined by $y^\ell = x^{a_1}(x-1)^{a_2}(x-\lambda)^{a_3}$ where $\ell, a_1, a_2, a_3 \in \mathbb{Z}_{>0}$, $(\ell, a_1, a_2, a_3) = 1$, $\alpha = a_1 + a_2 + a_3 \leq \ell$, $\ell \mid (q-1)$ and C_λ be a smooth model of X_λ. Then the genus of C_λ is calculated by the technique applied in Lemma 2.1.

Lemma 3.1. [2, (4)] *Let C be a smooth model of the curve X defined by $y^\ell = \prod_{j=1}^m (x - \mathfrak{q}_j)^{a_j}$. Denote $\alpha = \sum_{i=1}^m a_i$. Assume $(\ell, a_1, \dots, a_m) = 1$ and $\ell \geq \alpha$. Then*

$$g(C) = \frac{1}{2}\ell(m-1) - \frac{1}{2}\left\{\sum_{j=1}^m (\ell, a_j) + (\ell, \alpha)\right\} + 1,$$

where $(a, b) = \gcd(a, b)$.

Proof. If $a_j \geq 2$, X has a singularity at $\mathfrak{q}_j$. Then by blowing up there are (ℓ, a_j) points above $\mathfrak{q}_j$ with branch index $\ell/(\ell, a_j)$. Hence by the Hurwitz formula,

$$g(C) = 1 + \frac{(m-1)\ell}{2} - \frac{1}{2}\left\{\sum_{j=1}^m (\ell, a_j) + (\ell, \alpha)\right\}. \qquad \square$$

In our case the genus of C_λ is calculated by

$$g(C_\lambda) = \ell + 1 - \frac{1}{2}\left((\ell, a_1) + (\ell, a_2) + (\ell, a_3) + (\ell, \alpha)\right).$$

On the open set $U_{W_2=1} - \{0, 1, \lambda\}$ of C_λ, consider the differentials defined by

$$\omega_{k_1,k_2,k_3,k} = \frac{x^{k_1}(x-1)^{k_2}(x-\lambda)^{k_3}\,\mathrm{d}x}{y^k} \quad \text{and} \quad \omega_{r,k} = \frac{x^r\,\mathrm{d}x}{y^k}$$

which has the same form of $\omega_{r,s}$ introduced in the preceding section. (Recall (2.14): $k = \ell - 1 - s$.) Then we have the following technical lemma for later use.

Lemma 3.2. *There exists a basis $B = \{\omega_{k_1,k_2,k_3,k}\}$ such that the number*

$$M(k_1, k_3, k) = \left(\frac{(\alpha - a_2)}{\ell}k - (k_1 + k_3) - 1\right)(q-1) \tag{3.1}$$

is uniquely determined by k_1, k_3 and k. Denote B_k the subset of B containing the holomorphic differentials of the type $(*, *, *, k)$.

Proof. We will give an explicit algorithm to construct B in the appendix. $\square$

3.2. Proof of Theorem 1.2

We break the argument into three steps. The first step is to use the Lefschetz fixed-point theorem to get a rough idea of the shape of the summation. The second step is to examine the local behavior of each singular point and make necessary corrections, which we named correction functions. The last step is to calculate the number of rational points by the classical technique which we developed in the preceding sections. We can then determine the precise values of the constants according to the formulas derived in the first step.

Step 1*: Count rational points by the Lefschetz fixed-point theorem.*

Let us recall (2.6) and compute the number of rational points. Since a_1, a_2, a_3 might be greater than 1, there might be singularities at 0, 1, λ, ∞. Thus, we must take corrections on those points. Hence

$$1 - \operatorname{Tr}(F_b^*|_{H^1(C_\lambda,\mathcal{O})}) = \text{number of fixed points of } F_b \text{ on } C_\lambda,$$

which implies the number of rational points on X_λ is

$$|X_\lambda| = -\operatorname{Tr}(F_b^*|_{H^1(C_\lambda,\mathcal{O})}) - (\delta_\infty + \delta_0 + \delta_1 + \delta_\lambda),$$

where δ_0, δ_1, δ_λ are corrections at 0, 1, λ respectively and $\delta_\infty = |\text{points at } \infty| - 1$. Let $\delta = \delta_0 + \delta_1 + \delta_\lambda + \delta_\infty$. Then

$$|X_\lambda| \equiv \sum_{\omega_{k_1,k_2,k_3,k} \in B} -c_{k_1,k_2,k_3,k} \cdot F_{N_{k_1,k_2,k_3,k}} - \delta \mod p \tag{3.2}$$

for some constants $c_{k_1,k_2,k_3,k}$ and $N_{k_1,k_2,k_3,k}$.

Now we want to determine the corresponding parameters a, b, c for every differential $\omega_{k_1,k_2,k_3,k} \in B$. Recall the explicit expression of the differential $\omega_{k_1,k_2,k_3,k} \in B$:

$$\omega_{k_1,k_2,k_3,k} = x^{\left(k_1 - \frac{a_1 k}{\ell}\right)}(x-1)^{\left(k_2 - \frac{a_2 k}{\ell}\right)}(x-\lambda)^{\left(k_3 - \frac{a_3 k}{\ell}\right)}\,\mathrm{d}x.$$

By comparing with the differential $t^{b-1}(t-1)^{c-b-1}(t-\lambda)^{-a}\,\mathrm{d}t$,

$$a = \frac{a_3 k}{\ell} - k_3, \quad b = k_1 - \frac{a_1 k}{\ell} + 1, \quad c = k_1 + k_2 - \frac{a_1 k}{\ell} - \frac{a_2 k}{\ell} + 2$$

and

$$a' = -\sum_{j=1}^{3} k_j + \frac{\alpha k}{\ell} - 1, \quad b' = \frac{a_3 k}{\ell} - k_3, \quad c' = -k_1 - k_3 + \frac{a_1 k}{\ell} + \frac{a_3 k}{\ell}.$$

For simplicity, let $r = \sum_{j=1}^{3} k_j$, which plays a similar role as r defined in the previous case $y^\ell = x(x-1)(x-\lambda)$. Then we know the corresponding truncated hypergeometric serious is

$$-c_{k_1,k_2,k_3,k} F_{N_{k_1,k_2,k_3,k}}\left(\tfrac{\alpha k}{\ell} - r - 1, \tfrac{a_3 k}{\ell} - k_3, -k_1 - k_3 + \tfrac{a_1 k}{\ell} + \tfrac{a_3 k}{\ell}; \lambda\right), \tag{3.3}$$

where $c_{k_1,k_2,k_3,k}$ and $N_{k_1,k_2,k_3,k}$ are two constants to be determined and F can be either ${}_2F_{1,N}(a', b', c'; \lambda)$ or $\lambda^{(c'-1)(q-1)} \cdot {}_2F_{1,N}(a'-c'+1, b'-c'+1, -c'+2)$. Note that the exponent of λ in front of the hypergeometric series satisfies $(c'-1)(q-1) \equiv (1-c') \mod p$, which is consistent with the solution to the hypergeometric differential equations, and this is exactly the number M we introduced in (3.1).

Lemma 3.3. *Let* $N_{k_1,k_2,k_3,k} = (\frac{\alpha k}{\ell} - r - 1)(q-1)$ *and* $N'_{k_1} = (k_1 + 1 - \frac{a_1 k}{\ell})(q-1)$. *Let* $M = M(k_1, k_3, k)$ *be defined as in Lemma* 3.2. *If* $M < 0$, (k_1, k_2, k_3, k) *belongs to the regular parameters and the solution to the hypergeometric differential equation in* $\mathbb{F}_q$ *with parameters* (a', b', c') *is*

$$ {}_2F_{1,N_{k_1,k_2,k_3,k}}(a', b', c'; \lambda).$$

If $M \geq 0$, (k_1, k_2, k_3, k) *belongs to the irregular parameters and the solution to the differential equation in* $\mathbb{F}_q$ *is*

$$\lambda^M \cdot {}_2F_{1,N'_{k_1}}(a' - c' + 1, b' - c' + 1, -c' + 2; \lambda).$$

Proof. The only issue is the length of truncation. Since we are working on $\mathbb{F}_q$, either $(a')_n = 0$ in $\mathbb{F}_q$ or $(b')_n = 0$ in $\mathbb{F}_q$ can end the series. Note that for the first case, $a' + N_{k_1,k_2,k_3,k} = (\frac{\alpha k}{\ell} - r - 1)q \equiv 0$, so we can take it as the length of truncation. Similarly, for the second case, since $b' - c' + 1 = (k_1 + 1 - \frac{a_1 k}{\ell})$ we can take $(k_1 + 1 - \frac{a_1 k}{\ell})(q-1)$ as the length of truncation and it is precisely the value of N'_{k_1}. □

Step 2*: Compute the correction functions.*

In this step we generalize the correction terms defined in the last section, which is used to relate the number of rational points on X to the number of rational points on the normalization C. In general, the correction terms might depend on λ, which is different from the case in the last section. Thus instead of requiring a correction constant, we need a correction function $\delta(\lambda)$. By the defining equation of X_λ, there might be singular points along 0, 1, λ. Around $x = 0$, the defining equation of X_λ reads

$$y^\ell = x^{a_1}(-1)^{a_2}(-\lambda)^{a_3} + (\text{higher order terms}).$$

Let $d_1 = (\ell, a_1)$, then there are rational points on C_λ over $x = 0$ if and only if a d_1-th root of $(-1)^{a_2}(-\lambda)^{a_3}$ exists in $\mathbb{F}_q$. By (2.8), we want to design a function such that

$$\delta(1) = d_1 - 1, \quad \delta(\zeta^i) = -1 \quad \text{for } 1 \leq i \leq d_1 - 1.$$

This means if a d_1-th root of $(-1)^{a_2}(-\lambda)^{a_3}$ exists, there are d_1 rational points on C_λ and we must make a correction $d_1 - 1$. If a d_1-th root of $(-1)^{a_2}(-\lambda)^{a_3}$ does not exist, we must make a correction -1 because $(0, 0)$ is a rational point on X_λ.

Clearly, the function $\delta(r) = (1 + r + \cdots + r^{d_1 - 1}) - 1$ satisfies the properties we discussed above. Hence the correction function at $x = 0$ can be defined by

$$\delta_0(r) = \sum_{j=1}^{d_1 - 1} r^j, \tag{3.4}$$

where $d_1 = (\ell, a_1)$ and $r = ((-1)^{a_2}(-\lambda)^{a_3})^{(q-1)/d_1}$. By the same idea, we find that the local defining equations of X_λ around $x = 1$, $x = \lambda$ are

$$y^\ell = (x-1)^{a_2}(1-\lambda)^{a_3} \quad \text{and} \quad y^\ell = \lambda^{a_1}(\lambda-1)^{a_2}(x-\lambda)^{a_3},$$

and their associated correction functions are

$$\delta_1(s) = \sum_{j=1}^{d_2-1} s^j, \quad \delta_\lambda(t) = \sum_{j=1}^{d_3-1} t^j, \tag{3.5}$$

where $d_2 = (\ell, a_2)$, $a_3 = (\ell, a_3)$ and $s = ((1-\lambda)^{a_3})^{(q-1)/d_2}$, $t = (\lambda^{a_1}(\lambda-1)^{a_2})^{(q-1)/d_3}$. The singularity at infinity is simply $\delta_\infty = (\ell, \alpha)$, so the total correction function is

$$\delta = \delta_0 + \delta_1 + \delta_\lambda + \delta_\infty. \tag{3.6}$$

Lemma 3.4. *r^{κ_1}, s^{κ_2}, t^{κ_3} in* (3.4) *and* (3.5) *such that*

$$\kappa_i \cdot \frac{q-1}{d_i} = k, \quad 1 \le i \le 3$$

contribute to the weight-k counting of $|X_{\lambda,q}|$.

Proof. The proof is directly from construction. □

Then we can decompose δ with respect to the weight-k structure and write

$$\delta = \sum_k \sum_m \delta_{k,m}\, \lambda^m. \tag{3.7}$$

Note that the constant δ_∞ is at weight 0.

Step 3: Determine the constants.

Let us apply the classical technique again (cf. (2.10))

$$|X_\lambda| \equiv \sum_{x \in \mathbb{F}_q} (t + \cdots + t^{\ell-1}) \mod p.$$

Then

$$\begin{aligned} \sum_{x\in\mathbb{F}_q} t^k &= \sum_{x\in\mathbb{F}_q} x^{\frac{a_1 k(q-1)}{\ell}} \sum_m \binom{\frac{a_2 k(q-1)}{\ell}}{m} (-1)^m x^{\frac{a_2 k(q-1)}{\ell} - m} \\ &\quad \times \sum_n \binom{\frac{a_3 k(q-1)}{\ell}}{n} (-\lambda)^n x^{\frac{a_3 k(q-1)}{\ell} - n} \\ &= \sum_N (-1)^N \sum_{m+n=N} \binom{\frac{a_2 k(q-1)}{\ell}}{m} \binom{\frac{a_3 k(q-1)}{\ell}}{n} \lambda^n \cdot \sum_{x\in\mathbb{F}_q} x^{\frac{\alpha k(q-1)}{\ell} - N}. \end{aligned} \tag{3.8}$$

For brevity, we denote

$$N_2(k) = \frac{a_2 k(q-1)}{\ell}, \quad N_3(k) = \frac{a_3 k(q-1)}{\ell}. \tag{3.9}$$

By (2.9) the power of x is $\frac{\alpha k(q-1)}{\ell} - N = (r+1)(q-1)$ for some $r \in \mathbb{Z}_{\geq 0}$. Hence

$$N = N(k) = \left(\frac{\alpha k}{\ell} - r - 1\right)(q-1) \tag{3.10}$$

for some $r \in \mathbb{Z}_{\geq 0}$, and (3.8) can be simply written as

$$-\sum_{N}(-1)^N \sum_{m+n=N} \binom{N_2}{m}\binom{N_3}{n}\lambda^n.$$

By using the property of finite fields, we know that there are two relations in $\mathbb{F}_q$:

$$\lambda^{q-1} = 1 \quad \text{and} \quad 1 + \lambda + \cdots + \lambda^{q-2} = 1$$

for $\lambda \neq 0, 1$. Fixing k, the weight-k counting of $|X_{\lambda,q}|$ is

$$\begin{aligned} |X_{\lambda,q}|_{(k)} &\equiv -\sum_{N(k)}(-1)^N \sum_{m+n=N} \binom{N_2}{m}\binom{N_3}{n}\lambda^n \\ &\equiv \sum_{\omega_{k_1,k_2,k_3,k} \in B_k} -c_{k_1,k_2,k_3,k} F_{N_{k_1,k_2,k_3,k}}(a,b,c;\lambda) - \sum_m \delta_{k,m}\lambda^m \end{aligned} \tag{3.11}$$

in $\mathbb{F}_q$, where B_k is defined as in Lemma 3.2. According to the relations between N, N_2, N_3, there are four different types of summation. Fix k, then N_2, N_3 are fixed (cf. (3.9)).

Lemma 3.5. *Assume $0 < N \leq N_2 + N_3$, then*

(a) *for $N \leq N_2$, $N \leq N_3$,*

$$\sum_{n=0}^{N} \binom{N_2}{N-n}\binom{N_3}{n}\lambda^n = \binom{N_2}{N}\, {}_2F_{1,N}(-N, -N_3, 1-N+N_2; \lambda);$$

(b) *for $N_2 < N \leq N_3$,*

$$\sum_{n=0}^{N} \binom{N_2}{N-n}\binom{N_3}{n}\lambda^n = \binom{N_2}{N}\lambda^{N-N_2}\, {}_2F_{1,N_2}(-N_2, N-(N_2+N_3), N-N_2+1; \lambda);$$

(c) *for $N_3 < N \leq N_2$,*

$$\sum_{n=0}^{N} \binom{N_2}{N-n}\binom{N_3}{n}\lambda^n = \binom{N_2}{N}\, {}_2F_{1,N_3}(-N, -N_3, 1-N+N_2; \lambda);$$

(d) *for* $N_2 < N$, $N_3 < N$,

$$\sum_{n=0}^{N} \binom{N_2}{N-n}\binom{N_3}{n}\lambda^n = \binom{N_2}{N}\lambda^{N-N_2}\,{}_2F_{1,N_2+N_3-N}(-N_2, N-(N_2+N_3), N-N_2+1;\lambda).$$

Proof. These identities can be justified directly. □

We need to enumerate possible (k,r)s such that $\frac{\alpha k(q-1)}{\ell} \in \mathbb{Z}_{>0}$. This corresponds to δ_∞. If $d_\infty > 1$, we find the number of k satisfying $\frac{\alpha k}{\ell} - r - 1 \in \mathbb{Z}$ as we did in defining the correction in the case of $y^\ell = x(x-1)(x-\lambda)$. Let $\ell = \ell' d_\infty$ and $\alpha = \alpha' d_\infty$. Consider the condition

$$\frac{\alpha k}{\ell} - r - 1 = \frac{\alpha' k}{\ell'} - r - 1 \in \mathbb{Z}_{\geq 0} \implies k = \ell' k', \text{ and } k \text{ has to satisfy } \left\lceil \frac{\ell'}{\alpha'} \right\rceil \leq k \leq \ell - 1.$$

This implies $1 \leq k' \leq d_\infty - 1$ because if $k' = d_\infty \Rightarrow \alpha - r - 1 \geq 0$ which violates $r \leq \alpha - 2$. Therefore, the corrections is $d_\infty - 1$ which is exactly δ_∞, the correction at infinity.

Now we are ready to determine the constants $c_{k_1,k_2,k_3,k}$. The assumption $0 \leq N \leq N_2 + N_3$ implies

$$\min\left\{\left\lceil\frac{\alpha k}{\ell}\right\rceil - 1, \left\lceil\frac{a_2 k}{\ell}\right\rceil + (k_1+k_3)\right\} \geq r \geq \max\left\{\left\lceil\frac{a_1 k}{\ell}\right\rceil - 1, 0\right\},$$

and this gives the range of r for fixed k. Unlike the case of $y^\ell = x(x-1)(x-\lambda)$, the differential $\omega_{r,k}$ associated with the summation $\sum_{m+n=N}\binom{N_2}{m}\binom{N_3}{n}\lambda^n$ might not be holomorphic on X_λ. However, by Lemmas 3.2, 3.3 and (3.11), for each weight k, we know that there exist $\{c_{k_1,k_2,k_3,k}\}$ such that

$$|X_{\lambda,q}|_{(k)} + \sum_m \delta_{k,m}\lambda^m \equiv \sum_{\omega_{k_1,k_2,k_3,k} \in B_k} -c_{k_1,k_2,k_3,k} F_{N_{k_1,k_2,k_3,k}}(a,b,c;\lambda) \tag{3.12}$$

in $\mathbb{F}_q$, where $a = \frac{\alpha k}{\ell} - r - 1$, $b = \frac{a_3 k}{\ell} - k_3$, $c = -k_1 - k_3 + \frac{a_1 k}{\ell} + \frac{a_3 k}{\ell}$. This concludes the proof of Theorem 1.2.

3.3. Algorithm to find the coefficients

Let $G_k(\lambda) = |X_{\lambda,q}|_{(k)} + \sum_m \delta_{k,m}\lambda^m$. Then by the classical technique of taking derivatives we can generate enough equations to solve for $\{c_{k_1,k_2,k_3,k}\}$. Assuming $|B_k| = m$, we take derivatives with respect to λ and get a system of equations

$$\begin{aligned} G_k(\lambda) &= \sum -c_{k_1,k_2,k_3,k} F_{N_{k_1,k_2,k_3,k}}(a,b,c;\lambda), \\ G_k'(\lambda) &= \sum -c_{k_1,k_2,k_3,k} F'_{N_{k_1,k_2,k_3,k}}(a,b,c;\lambda), \\ &\vdots \\ G_k^{(m-1)}(\lambda) &= \sum -c_{k_1,k_2,k_3,k} F^{(m-1)}_{N_{k_1,k_2,k_3,k}}(a,b,c;\lambda). \end{aligned} \tag{3.13}$$

By Lemma 3.5, we have $G_k(\lambda) = f_1 + \cdots + f_n$ where $f_i = C_i\,{}_2F_{1,N_i}(a,b,c;\lambda)$ or $f_i = C_i\lambda^{(c-1)}\,{}_2F_{1,N_i}(a,b,c;\lambda)$ for every i. Let $g_1, g_2, \ldots, g_m$ be the vectors of functions on the right-hand side of (3.13). Each entry of g_j has the form ${}_2F_{1,N_j}(a',b',c';\lambda)$ or $\lambda^{(c'-1)(q-1)}$ ${}_2F_{1,N_j}(a'-c'+1, b'-c'+1, -c'+2;\lambda)$. Let $c_1, \ldots, c_m$ be the unknowns and G_k be the column vector $(G_k(\lambda), G_k'(\lambda), \ldots, G_k^{m-1}(\lambda))^T$. Then, by Cramer's rule one has

$$c_j = \frac{W[g_1, \ldots, G_k, \ldots, g_m]}{W[g_1, \ldots, g_m]} = \text{constant},$$

where W represents the Wronskian. Thus we can introduce any number into λ. For simplicity, we can set $\lambda = 1$. Notice that f_i and g_j have the form $\lambda^M F_N(a,b,c;\lambda)$ and the derivative of a hypergeometric series with respect to λ is

$$F_N'(a,b,c;\lambda) = \frac{ab}{c} F_{N-1}(a+1, b+1, c+1;\lambda).$$

This implies

$$\begin{aligned}
&(\lambda^M F_N(a,b,c;\lambda))^{(s)}\Big|_{\lambda=1} \\
&= C_s^s(\lambda^M)^{(s)} + C_{s-1}^s(\lambda^M)^{(s-1)}F_N'(a,b,c;\lambda) + \cdots\Big|_{\lambda=1} \\
&= \sum_{j=0}^{s} C_{s-j}^s\,(M\cdots(M-s+j+1))\,\frac{(a)_j(b)_j}{(c)_j}F_{N-j}(a+j, b+j, c+j;1) \\
&= \sum_{j=0}^{s} \frac{(-s)_{s-j}(-M)_{s-j}(a)_j(b)_j}{(c)_j\,j!}F_{N-j}(a+j, b+j, c+j;1).
\end{aligned}$$

Apply this formula to every $f_i^{(s)}$ and $g_j^{(s)}$, $1 \le s \le m-1$ and we get an explicit expression of coefficients in (3.12).

4. Remarks on the Legendre family of elliptic curves over $\mathbb{F}_q$

The results of Section 2 in the case of $\ell = 2$ and $q = p$ give rise to the classically known results for the Legendre family of elliptic curves. In the case of $q = p^n$ with $n > 1$, apart from the method presented in Section 2, one can also obtain a similar expression by a classical approach of considering a truncated hypergeometric series related to p instead of p^n. The goal of this section is to show that after applying Weil's results on the number of rational points over a finite field the two countings with different truncated hypergeometric series are actually the same.

4.1. Arithmetic geometry

Let us first generalize the classical arguments in counting. There are two steps in this argument. The first step is to apply Fermat's little theorem to count the numbers of

rational points directly:

$$|E_\lambda| \equiv \sum_{x\in\mathbb{F}_p} \left(1 + (x(x-1)(x-\lambda))^{(p-1)/2}\right) \mod p. \tag{4.1}$$

Here we follow the same guild line. On the finite field $\mathbb{F}_q$, the identity

$$a^{q-1} \equiv 1$$

for $a \in \mathbb{F}_q^*$ holds. By the construction of $\mathbb{F}_q$, we have a criterion of quadratic roots:

$$a^{(q-1)/2} \equiv \begin{cases} 1 & \text{if there exists } y \text{ such that } a = y^2, \\ -1 & \text{otherwise,} \end{cases}$$

which is a special case of (2.8). Hence we have

$$|E_\lambda| \cdot 1 \equiv \sum_{x\in\mathbb{F}_q} \left(1 + (x(x-1)(x-\lambda))^{(q-1)/2}\right) \quad \text{in } \mathbb{F}_q.$$

By (2.9) we can conclude

$$|E_\lambda| \cdot 1 \equiv -(-1)^{(q-1)/2} \sum_{r=0}^{(q-1)/2} \binom{-1/2}{r}^2 \lambda^r \quad \text{in } \mathbb{F}_q, \tag{4.2}$$

which implies

$$\begin{aligned} |E_{\lambda,q}| &\equiv -(-1)^{(q-1)/2} \sum_{r=0}^{(q-1)/2} \binom{-1/2}{r}^2 \lambda^r \mod p \\ &\equiv -(-1)^{(q-1)/2} {}_2F_{1,(q-1)/2}(\tfrac{1}{2},\tfrac{1}{2},1;\lambda). \end{aligned} \tag{4.3}$$

For the interpretation, recall the Picard-Fuch equation

$$\begin{aligned} &\left(\frac{1}{4} + (2\lambda-1)\frac{\partial}{\partial\lambda} + \lambda(\lambda-1)\frac{\partial^2}{\partial\lambda^2}\right) a_{p-1}(\lambda)(x-x(\mathfrak{q}))^{p-1} \\ \equiv\ & \frac{-1}{2}\frac{\mathrm{d}}{\mathrm{d}x}\left(c_p(\lambda)(x-x(\mathfrak{q}))^p\right) \equiv 0 \end{aligned} \tag{4.4}$$

over $\mathbb{F}_q$, where $q = p^n$. On $\mathbb{F}_q$, the Frobenius map is $F(x) = x^q$. Therefore, we only have to replace p by q and get

$$\begin{aligned} &|E_\lambda| \equiv -a_{q-1}(\lambda) \equiv -k \cdot \sum_{r=0}^{(q-1)/2} \binom{-1/2}{r}^2 \lambda^r \quad \text{in } \mathbb{F}_q \\ \implies\ &|E_\lambda| \equiv -k \cdot {}_2F_{1,(q-1)/2}(\tfrac{1}{2},\tfrac{1}{2},1;\lambda) \mod p. \end{aligned} \tag{4.5}$$

Let us explain the first identity. Since a_{q-1} satisfies (4.4), a_{q-1} has a series expression

$$a_{q-1} = \sum_{k=0}^{q-1} c_k \lambda^k.$$

This is because $\mathbb{F}_q$ has q elements which implies that the upper bound of the summation is $q-1$. Another explanation is by Fermat's little theorem, which says $\lambda^q = \lambda$ for every λ. Hence the highest meaningful power of λ is $q-1$. Then, through the explicit solution of the hypergeometric differential equation, we have

$$a_{q-1} \equiv k \sum_{r=0}^{(q-1)/2} \binom{-1/2}{r}^2 \lambda^r \quad \text{in } \mathbb{F}_q. \tag{4.6}$$

By comparing (4.2), (4.5) and (4.6), we have $k \equiv (-1)^{(q-1)/2}$ in $\mathbb{F}_q$, which implies that k can be taken as an integer and

$$k \equiv (-1)^{(q-1)/2} \mod p.$$

Therefore by (4.2), (4.3) and (4.6) we can conclude

Proposition 4.1.

$$|E_{\lambda,q}| \equiv -a_{q-1}(\lambda) \equiv -(-1)^{(q-1)/2} \cdot {}_2F_{1,(q-1)/2}(\tfrac{1}{2}, \tfrac{1}{2}, 1; \lambda) \tag{4.7}$$

for every $q = p^n$.

4.2. Computation after Weil

Let us approach the same problem by Weil's conjecture/theorem on smooth algebraic curves. By using Tate's module or Étale cohomology one can derive

$$\begin{aligned} \#E(\mathbb{F}_q) &= 1 - \alpha^n - \beta^n - p^n \\ &\equiv 1 - (\alpha^n + \beta^n) \mod p, \end{aligned} \tag{4.8}$$

where $\beta = \overline{\alpha}$ and $|\alpha| = |\beta| = \sqrt{q}$ (cf. [5, p. 136]). Let $a = (\alpha + \beta) \in \mathbb{Z}$. Note that the notation $\#E(\mathbb{F}_q)$ includes the infinity point. Thus by our notation we have

$$\#E_\lambda(\mathbb{F}_q) = 1 + |E_{\lambda,q}|\,.$$

We can calculate a by letting $n = 1$ and comparing with (1.1), which implies

$$a \equiv (-1)^{(p-1)/2} {}_2F_{1,(p-1)/2}(\tfrac{1}{2}, \tfrac{1}{2}, 1; \lambda) \mod p.$$

To abbreviate, we denote $F = {}_2F_{1,p/2}(\frac{1}{2}, \frac{1-p}{2}, 1; \lambda)$. Then we can derive $|E_{\lambda,q}|$ for $n \geq 1$ by a simple observation

$$\alpha^n + \beta^n \equiv (\alpha + \beta)^n \equiv a^n \mod p.$$

Proof. The key is to show $\alpha^n + \beta^n \in \mathbb{Z}$. We will prove this by induction on n. The case of $n = 1$ is obvious. For the general case, according to the binomial expansion

$$\begin{aligned}(\alpha+\beta)^n &= \sum_{k=0}^{n} C_k^n \alpha^{n-k}\beta^k \\ &= (\alpha^n+\beta^n) + C_1^n\alpha\beta(\alpha^{n-2}+\beta^{n-2}) + \cdots,\end{aligned} \tag{4.9}$$

and then by the induction hypothesis $C_1^n\alpha\beta(\alpha^{n-2}+\beta^{n-2})+\cdots \in \mathbb{Z}$, we can conclude that $\alpha^n + \beta^n \in \mathbb{Z}$. Again by (4.9), since $\alpha\beta = |\alpha|^2 = q$,

$$\begin{aligned}(\alpha+\beta)^n &= (\alpha^n+\beta^n) + q\left(C_1^n(\alpha^{n-2}+\beta^{n-2})+\cdots\right) \\ &\equiv (\alpha^n+\beta^n) \mod p.\end{aligned}$$

□

Therefore we can calculate

$$\begin{aligned}\#E_\lambda(\mathbb{F}_q) &\equiv 1-(\alpha^n+\beta^n) \equiv 1-a^n \mod p \\ &\equiv 1-\left((-1)^{(p-1)/2}F\right)^n \mod p \\ \implies |E_{\lambda,q}| &\equiv -(-1)^{(p-1)n/2}F^n \mod p.\end{aligned}$$

It is easy to verify

$$(-1)^{(p-1)n/2} = (-1)^{(p^n-1)/2},$$

so we get an equation

$$\sum_{r=0}^{(q-1)/2}\binom{-1/2}{r}^2\lambda^r \equiv \left(\sum_{r=0}^{(p-1)/2}\binom{-1/2}{r}^2\lambda^r\right)^n \mod p. \tag{4.10}$$

Remark 4.2. Incidentally, this equation leads to the following non-obvious identity:

$${}_2F_{1,(q-1)/2}(\tfrac{1}{2},\tfrac{1}{2},1;\lambda) \equiv \left({}_2F_{1,(p-1)/2}(\tfrac{1}{2},\tfrac{1}{2},1;\lambda)\right)^n \mod p.$$

5. Examples

5.1.

In this subsection, we will use examples to illustrate subtleties between taking modulo p and modulo $q = p^n$ for $n > 1$, which explains why Theorem 1.1 was stated in terms of (mod p) instead of (mod q).

Example 5.1. Let X_λ^2 be defined by $y^2 = x(x-1)(x-\lambda)$ and p be a prime. Let $q = p^n$. Recall the formula (4.7)

$$F_{\lambda,q}^2 = -(-1)^{(q-1)/2}\cdot {}_2F_{1,(q-1)/2}(\tfrac{1}{2},\tfrac{1}{2},1;\lambda).$$

Let $\lambda = 3$, then

- $q = 5$, then $\left|X^2_{3,5}\right| = 3$ and $F^2_{3,5} \equiv 3 \mod 5$.
- $q = 5^2$, then $\left|X^2_{3,5^2}\right| = 31$ and $F^2_{3,5^2} \equiv 1 \mod 5$, $F^2_{3,5^2} \equiv 6 \mod 5^2$.
- $q = 5^3$, then $\left|X^2_{3,5^3}\right| = 147$ and $F^2_{3,5^3} \equiv 2 \mod 5$, $F^2_{3,5^3} \equiv 97 \mod 5^3$.

These three results shows that taking modulo p is necessary. The identities will be failed if one takes modulo $q = p^n$.

Example 5.2. Let X^4_λ be defined by $y^4 = x(x-1)(x-\lambda)$ and p be a prime. Let $q = p^n$. By using Theorem 1.1, we have

$$F^4_{\lambda,q} = -k_1\lambda^{(q-1)/2}F_{N_1}(\tfrac{1}{4}, \tfrac{3}{4}, \tfrac{1}{2}; \lambda) - k_2F_{N_2}(\tfrac{1}{4}, \tfrac{3}{4}, \tfrac{1}{2}; \lambda) - k_3F_{N_3}(\tfrac{1}{2}, \tfrac{1}{2}, 1; \lambda),$$

where

$$k_1 = (-1)^{5(q-1)/4}\binom{\frac{3(q-1)}{4}}{\frac{2(q-1)}{4}}, \quad k_2 = (-1)^{(q-1)/4}\binom{\frac{3(q-1)}{4}}{\frac{(q-1)}{4}}, \quad k_3 = (-1)^{(q-1)/2},$$
$$N_1 = \frac{q-1}{4}, \quad N_2 = \frac{q-1}{4}, \quad N_3 = \frac{q-1}{2}.$$

Let $\lambda = 3$, then

- $q = 5$, then $\left|X^4_{3,5}\right| = 3$ and $F^4_{3,5} \equiv 3 \mod 5$.
- $q = 5^2$, then $\left|X^4_{3,5^2}\right| = 19$ and $F^4_{3,5^2} \equiv 4 \mod 5$, $F^4_{3,5^2} \equiv 14 \mod 5^2$.
- $q = 5^3$, then $\left|X^4_{3,5^3}\right| = 147$ and $F^4_{3,5^3} \equiv 2 \mod 5$, $F^4_{3,5^3} \equiv 17 \mod 5^3$.
- $q = 17$, then $\left|X^4_{3,17}\right| = 23$ and $F^4_{3,17} \equiv 6 \mod 17$.
- $q = 7$, then $\left|X^4_{3,7}\right| = 3$ and $F^2_{3,7} \equiv 3 \mod 7$.
- $q = 11$, then $\left|X^4_{3,11}\right| = 15$ and $F^2_{3,11} \equiv 4 \mod 11$.

The first three results shows that taking modulo p is necessary. The identities will be failed if one takes modulo $q = p^n$. For $q = 5^n$, 17, they satisfy the assumption $(m, q-1) = 4$ (where $m = \ell = 4$). For the last two identities, they satisfy the assumption $(m, q-1) = 2$ (where $m = 4$, $\ell = 2$).

5.2.

The following example shows that the assumption of $\ell = (m, q-1)$ in Theorem 1.1 is necessary.

Example 5.3. Let X^6_λ be defined by $y^6 = x(x-1)(x-\lambda)$. As before, we denote $F^6_{\lambda,q}$ the formula provided in Theorem 1.1. Let $F'^6_{\lambda,q} = F^6_{\lambda,q} - \delta$, i.e., without considering the correction terms. Let $\lambda = 3$, then

- $q = 7$, then $\left|X^6_{3,7}\right| = 3$ and $F'^6_{3,7} \equiv 5 \mod 7$.
- $q = 13$, then $\left|X^6_{3,13}\right| = 27$ and $F'^6_{3,13} \equiv 3 \mod 13$.
- $q = 17$, then $\left|X^6_{3,17}\right| = 23$ and $F^6_{3,17} \equiv 4 \mod 17$, $F^2_{3,17} \equiv 6 \mod 17$.

The first two results shows that the correction terms are necessary. For the last result, the formula $F^6_{\lambda,q}$ does not provide the correct result in the case $6 \nmid (17-1)$. Instead, we must consider the right power and do the reduction: $F^2_{\lambda,q}$ where $2 = (6, 17-1)$.

6. Appendix

We will present an explicit algorithm mentioned in the proof of Lemma 3.2. First let us recall:

Lemma 6.1. [2, Theorem 3] *$\omega_{k_1,k_2,k_3,k}$ is holomorphic if and only if (k_1, k_2, k_3, k) satisfies*

- Test1: *$\ell(k_j + 1) \geq k a_j + (\ell, a_j)$ for $j = 1, 2, 3$, and*
- Test2: *$k\alpha \geq (k_1 + k_2 + k_3 + 1)\ell + (\ell, \alpha)$.*

Now we declare variables m $= \ell$, a $= \alpha$, k1 $= k_1$, k2 $= k_2$, k3 $= k_3$. Then we have the following algorithm.

Listing 1: Find a basis

```
for(k=IntgerPart(m/a)+1; k<=m-1; k++){
        n=-1; // control flag.
        for(k3=0; k3<=a-2; k3++){
        for(k2=0; k2<=a-2; k2++){
        for(k1=0; k1<=a-2 && k1+k2+k3>n; k1++){
                Test1;
                Test2;
                n=k1+k2+k3; // reset the flag.
        }}}
}
```

Note that for each fixed k, we move k3 first, then k2, then k1. In this manner we can make k1 + k2 + k3 keep growing. One can easily justify that this feature makes B satisfy the requirement in Lemma 3.2.

Acknowledgments

We want to specially thank Professor Sai-Kee Yeung for useful discussion and generous advice on this paper.

References

[1] C. H. Clemens, *A Scrapbook of Complex Curve Theory*, Second edition, Graduate Studies in Mathematics **55**, American Mathematical Society, Providence, RI, 2003. https://doi.org/10.1090/gsm/055

[2] J. K. Koo, *On holomorphic differentials of some algebraic function field of one variable over* $\mathbb{C}$, Bull. Austral. Math. Soc. **43** (1991), no. 3, 399–405. https://doi.org/10.1017/s0004972700029245

[3] Ju. I. Manin, *Algebraic curves over fields with differentiation*, Amer. Math. Soc. Transl. Ser. 2 **37** (1964), 59–78. https://doi.org/10.1090/trans2/037/07

[4] ———, *The Hasse-Witt matrix of an algebraic curve*, Amer. Math. Soc. Transl. Ser. 2 **45** (1965), 245–264. https://doi.org/10.1090/trans2/045/16

[5] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Second edition, Graduate Texts in Mathematics **106**, Springger, Dordrecht, 2009. https://doi.org/10.1007/978-0-387-09494-6

Yih Sung
Department of Mathematics, University of Wisconsin-Madison, Van Vleck Hall, 480 Lincoln Drive, Madison, WI 53706, USA
E-mail address: ysung26@wisc.edu