Counting matrix points on certain varieties over finite fields

Yifeng Huang, Ken Ono, and Hasan Saad

Abstract. Classical hypergeometric functions are well-known to play an important role in arithmetic algebraic geometry. These functions offer solutions to ordinary differential equations, and special cases of such solutions are periods of Picard-Fuchs varieties of Calabi-Yau type. Gauss' ${}_2F_1$ includes the celebrated case of elliptic curves through the theory of elliptic functions. In the 1980s, Greene defined finite field hypergeometric functions, and these functions can be used to enumerate the number of finite field points on such varieties. We extend some of these results to count finite field "matrix points." For example, we consider the matrix elliptic curves

$$B^2 = A(A - I_n)(A - aI_n),$$

where (A, B) are commuting $n \times n$ matrices over a finite field $\mathbb{F}_q$ and $a \neq 0, 1$ is fixed. These formulas are assembled from Greene's hypergeometric functions and q-multinomial coefficients.

1. Introduction and Statement of Results

Classical hypergeometric functions are well known to give periods of elliptic curves. To be precise, if n is a nonnegative integer, then define $(\gamma)_n$ by

$$(\gamma)_n := \begin{cases} 1 & \text{if } n = 0, \\ \gamma(\gamma+1)(\gamma+2)\cdots(\gamma+n-1) & \text{if } n \geq 1. \end{cases}$$

The *classical hypergeometric function* in parameters $\alpha_1, \ldots, \alpha_h, \beta_1, \ldots, \beta_j \in \mathbb{C}$ is defined by

$${}_hF_j^{\mathrm{cl}}\left(\begin{matrix}\alpha_1 & \alpha_2 & \ldots & \alpha_h \\ & \beta_1 & \ldots & \beta_j\end{matrix}\;\middle|\; x\right) := \sum_{n=0}^{\infty} \frac{(\alpha_1)_n(\alpha_2)_n(\alpha_3)_n\cdots(\alpha_h)_n}{(\beta_1)_n(\beta_2)_n\cdots(\beta_j)_n} \cdot \frac{x^n}{n!}.$$

Perhaps the most famous example illustrating the role of these functions in geometry involves the Legendre elliptic curves

$$E_{\mathrm{L}}(a): \quad y^2 = x(x-1)(x-a), \qquad a \in \mathbb{C} \setminus \{0, 1\}. \tag{1.1}$$

The theory of elliptic integrals shows, for $0 < a < 1$, that the function ${}_2F_1^{\mathrm{cl}}(x) := {}_2F_1^{\mathrm{cl}}\left(\begin{matrix}\frac{1}{2} & \frac{1}{2} \\ & 1\end{matrix}\;\middle|\; x\right)$ (for example, see page 184 of [**10**]) gives the real period $\Omega_{\mathrm{L}}(a)$ of $E_{\mathrm{L}}(a)$ by the formula

$$\Omega_{\mathrm{L}}(a) = \pi \cdot {}_2F_1^{\mathrm{cl}}(a). \tag{1.2}$$

There is another kind of hypergeometric function, the finite field hypergeometric function, that gives further information about these elliptic curves and higher dimensional varieties. These functions count points over finite fields. To make this precise, we first recall their definition which

2020 *Mathematics Subject Classification.* 33C70; 14Gxx.

Key words and phrases. Hypergeometric functions, Matrix points, Elliptic curves, $K3$ surfaces.

Y.H. thanks the AMS–Simons Travel Grant for making this collaboration possible.

K.O. thanks the Thomas Jefferson Fund and the NSF (DMS-2002265 and DMS-2055118) for their support.

is due to Greene [**7**]. If q is a prime power and A and B are two Dirichlet characters on $\mathbb{F}_q$ (extended so that $A(0)=B(0)=0$), then let $\binom{A}{B}$ be the normalized Jacobi sum

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

Here $\overline{B}$ is the complex conjugate of B. If $A_0, \ldots, A_n$, and $B_1, \ldots, B_n$ are characters on $\mathbb{F}_q$, then the *finite field hypergeometric function* in these parameters is defined by

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

Here $\sum_\chi$ denotes the sum over all characters χ of $\mathbb{F}_q$.

It has been observed by many authors (see [**7**], [**8**], [**11**], [**12**], [**15**], and [**17**], to name a few) that the Gaussian analog of a classical hypergeometric series with rational parameters is obtained by replacing each $\frac{1}{n}$ with a character χ_n of order n (and $\frac{a}{n}$ with χ_n^a). Let ϵ_q be the trivial character on $\mathbb{F}_q$ and let ϕ_q be the character of order 2. Then the finite field analog of ${}_2F_1^{\mathrm{cl}}(x)$ is

$${}_2F_1^{\mathrm{ff}}(x)_q := \left(\begin{matrix} \phi_q & \phi_q \\ & \epsilon_q \end{matrix} \,\middle|\, x\right)_q.$$

More generally, we let

$$\tag{1.3} {}_{n+1}F_n^{\mathrm{ff}}(x)_q := {}_{n+1}F_n^{\mathrm{ff}}\left(\begin{matrix} \phi_q & \phi_q & \ldots \phi_q \\ & \epsilon_q & \ldots \epsilon_q \end{matrix} \,\middle|\, x\right)_q.$$

M. Koike proved [**12**] that if $p \geq 5$ is a prime for which $E_{\mathrm{L}}(a)$ has good reduction, and q is a power of p, then

$$\tag{1.4} {}_2F_1^{\mathrm{ff}}(a)_q = -\frac{\phi_q(-1)}{q} \cdot a_{\mathrm{L}}(a;q),$$

where $q+1-a_{\mathrm{L}}(a;q)$ counts the number of $\mathbb{F}_q$-points on $E_{\mathrm{L}}(a)$. This expression is the finite field analogue of Gauss' period formula (1.2).

Motivated by (1.2) and (1.4), it is natural to ask whether other finite field hypergeometric function evaluations give point counts for other varieties. This is indeed the case, and perhaps the most beautiful example involves the analog of the celebrated classical Clausen identity [**4**]

$$\tag{1.5} {}_3F_2^{\mathrm{cl}}\left(\begin{matrix} b+c & 2b & 2c \\ & b+c+\frac{1}{2} & 2b+2c \end{matrix} \,\middle|\, x\right) = {}_2F_1^{\mathrm{cl}}\left(\begin{matrix} b & c \\ & b+c+\frac{1}{2} \end{matrix} \,\middle|\, x\right)^2.$$

Using this identity, D. McCarthy [**13**] proved that if $a > 0$, then

$${}_3F_2^{\mathrm{cl}}\left(\begin{matrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ & 1 & 1 \end{matrix} \,\middle|\, \frac{a}{a+1}\right) = \frac{\sqrt{1+a}}{\pi^2} \cdot \Omega_{CL}(a)^2,$$

where $\Omega_{CL}(a)$ is the real period of the Clausen elliptic curve

$$E_{CL}(a): \quad y^2 = (x-1)(x^2+a).$$

In the finite field case, the second author proved that if $\mathbb{F}_q$ is a finite field of characteristic $\mathrm{char}(\mathbb{F}_q) \geq 5$ and $a \in \mathbb{F}_q \setminus \{0,1\}$, then

$$\tag{1.6} q + q^2\phi_q(a+1) \cdot {}_3F_2^{\mathrm{ff}}\left(\frac{a}{a+1}\right)_q = a_{CL}(a;q)^2 = -\phi_q(1+\sqrt{-a}) \cdot q \cdot {}_2F_1^{\mathrm{ff}}\left(\frac{1-\sqrt{-a}}{1+\sqrt{-a}}\right)_q,$$

where $q+1-a_{CL}(a;q)$ is the number of $\mathbb{F}_q$ points on $E_{CL}(a)$, and where the second equality holds whenever $-a$ is a square in $\mathbb{F}_q$. This equality is an analogue of a special case of Clausen's identity. Furthermore, this identity can be interpreted in terms of $K3$ surfaces whose function fields are given by

$$X_a: \quad s^2 = xy(x+1)(y+1)(x+ay),$$

where $a \in \mathbb{F}_q \setminus \{0, -1\}$. In this notation, it is known (see Theorem 11.18 of [**14**] and Proposition 4.1 of [**1**]) that

$$|X_a(\mathbb{F}_q)| = 1 + q^2 + 19q + q^2 \cdot {}_3F_2^{\mathrm{ff}}(-a)_q. \tag{1.7}$$

In this note we show that the hypergeometric identities (1.4) and (1.7), combined with the combinatorial input from partitions and q-multinomial coefficients, count suitable "matrix points" on these curves and surfaces. To make this precise, we first introduce some notation. If n, m are positive integers and K is a field, then let $C_{n,m}(K)$ denote the set of pairwise-commuting m-tuples of $n \times n$-matrices over K. Due to the noncommutativity of matrix multiplication, geometric problems related to studying matrix rational points on curves and higher varieties only make sense when the matrices are commuting, that is, when the matrix points are in $C_{n,m}(K)$. We will be interested in counting tuples in $C_{n,m}(K)$ which satisfy the equations defining some affine varieties. More precisely, we will consider the sets

$$\{(A, B) \in C_{n,2}(\mathbb{F}_q) : B^2 = A(A - I_n)(A - aI_n)\}$$

and

$$\{(A, B, C) \in C_{n,3}(\mathbb{F}_q) : C^2 = AB(A + I_n)(B + I_n)(A + aB)\}$$

as matrix analogues of the Legendre elliptic curves E_{L} and the K3 surfaces X_a considered above.

To express our results, we introduce some notation. If λ is a partition of a nonnegative integer k, we write $n(\lambda; i)$ to denote the number of times i is repeated in λ. Furthermore, we write $|\lambda| = k$, and write $l(\lambda) = \sum n(\lambda; i)$ to denote the number of parts of λ. Additionally, we introduce certain polynomials in q. More precisely, if z and q are any complex numbers, and n is any positive integer, then we define the q-Pochhammer symbol

$$(z; q)_n := (1 - z)(1 - zq) \dots (1 - zq^{n-1}) \tag{1.8}$$

with $(z; q)_0 = 1$. Finally, for an integer $n \geq 0$ and $m_1 + \ldots + m_n = n$ a partition of n, we define the q-multinomial factor

$$\binom{n}{m_1, m_2, \dots, m_n}_q := \frac{(q; q)_n}{(q; q)_{m_1}(q; q)_{m_2} \dots (q; q)_{m_n}}.$$

It is known that $\binom{n}{m_1,\dots,m_n}_q$ is a monic polynomial in q and that $\binom{n}{m_1,\dots,m_n}_q$ approaches the usual multinomial coefficient as $q \to 1$.

We start by expressing the number of commuting matrices on a Legendre elliptic curve. More precisely, if n is a positive integer, q is a prime power and $a \in \mathbb{F}_q$, we let

$$N_{n,2}(a; q) := |\{(A, B) \in C_{n,2}(\mathbb{F}_q) : B^2 = A(A - I_n)(A - aI_n)\}|. \tag{1.9}$$

In this notation, we have the following theorem that determines these counts, and also explains the connection with the classical ${}_2F_1^{\mathrm{cl}}$-hypergeometric function.

Theorem 1.1. *If $q = p^r$ is a prime power with $p \geq 5$ and $a \in \mathbb{F}_q \setminus \{0, 1\}$, then*

$$N_{n,2}(a; q) = \sum_{k=0}^{n} \phi_{q^k}(-1) \cdot P(n, k)_q \cdot {}_2F_1^{\mathrm{ff}}(a)_{q^k},$$

where

$$P(n, k)_q = (-1)^k q^{n(n-k) + \frac{k(k+1)}{2}} \sum_{s=0}^{\lfloor \frac{n-k}{2} \rfloor} q^{2s(s-n+k)} \binom{n}{s, n-k-2s, k+s}_q.$$

Moreover, $P(n, k)_q$ is a polynomial in q with leading term $(-1)^k \cdot q^{n^2 - \frac{k(k-1)}{2}}$ and

$$\lim_{q \to 1} P(n, k)_q = (-1)^k \binom{n}{k} \cdot {}_2F_1^{\mathrm{cl}} \left(\begin{matrix} \frac{k-n}{2} & \frac{k+1-n}{2} \\ & k+1 \end{matrix} \,\middle|\, 4 \right).$$

As a corollary, we consider the matrix analog of the Sato–Tate distribution for point counts for elliptic curves over finite fields. In direct analogy, we find that the limiting distribution of the "random part" of matrix point counts on Legendre elliptic curves is semicircular. More precisely, if n is a positive integer and q is a prime power, then we let

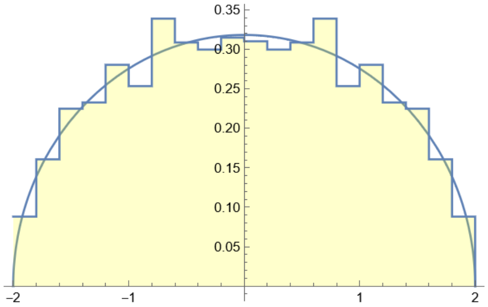
$$a_{\mathrm{L},n}(a;q) := N_{n,2}(a;q) - P(n,0)_q. \tag{1.10}$$

In this notation, we have the following result.

Corollary 1.2. *If $-2 \leq b < c \leq 2$ and n and r are fixed positive integers, then we have*

$$\lim_{p\to\infty} \frac{|\{a \in \mathbb{F}_{p^r} : p^{\frac{r}{2}-rn^2} a_{\mathrm{L},n}(a;p^r) \in [b,c]\}|}{p^r} = \frac{1}{2\pi}\int_b^c \sqrt{4-t^2}dt.$$

Example 1.3. For the prime $p = 93283$, we compare the histogram of the distribution of $p^{-7/2}a_{L,2}(a;p)$ for $a \in \mathbb{F}_p$ with the limiting distribution.



$p^{-7/2}a_{L,2}(a;p)$ histogram for $p = 93283$

We also consider the matrix version of the $K3$ surfaces described above. If n is a positive integer, q is a prime power, and $a \in \mathbb{F}_q$, then we let

$$N_{n,3}(a;q) := |\{(A,B,C) \in C_{n,3}(\mathbb{F}_q) : C^2 = AB(A+I_n)(B+I_n)(A+aB)\}|. \tag{1.11}$$

In this notation, we have the following theorem that gives matrix point counts in terms of the ${}_3F_2^{\mathrm{ff}}$-hypergeometric function, 4-tuples of integer partitions, and q-multinomial coefficients.

Theorem 1.4. *If $q = p^r$ is a prime power with $p \geq 5$ and $a \in \mathbb{F}_q \setminus \{0,-1\}$, then we have*

$$N_{n,3}(a;q) = R(n,\phi_q(a+1))_q + \sum_{k=0}^{n} Q\left(n,k,\phi_q(a+1)\right)_q \cdot {}_3F_2^{\mathrm{ff}}\left(\frac{a}{a+1}\right)_{q^k},$$

where

$$Q(n,k,\gamma)_q := q^{\frac{n(n-1)}{2}+k} \sum_{\substack{\lambda_1,\ldots,\lambda_4 \\ |\lambda_1|+\ldots+|\lambda_4|=n \\ l(\lambda_3)-l(\lambda_4)=k}} q^{l(\lambda_1)}\gamma^{l(\lambda_2)}(-1)^{n-m(\lambda_1,\ldots,\lambda_4)}$$
$$(q,q)_{n-m(\lambda_1,\ldots,\lambda_4)} \cdot q^{\sum\frac{n(\lambda_i,j)(n(\lambda_i,j)+1)}{2}} \cdot \binom{n}{n(\lambda_i,j),\, n-m(\lambda_1,\ldots,\lambda_4)}_q$$

and

$$R(n,\gamma)_q := -\, q^{\frac{n(n-1)}{2}} \cdot \sum_{\substack{\lambda_1,\ldots,\lambda_4 \\ |\lambda_1|+\ldots+|\lambda_4|=n \\ l(\lambda_3)\neq l(\lambda_4)}} q^{l(\lambda_1)}\gamma^{l(\lambda_2)+l(\lambda_3)-l(\lambda_4)}(-1)^{n-m(\lambda_1,\ldots,\lambda_4)}$$
$$(q,q)_{n-m(\lambda_1,\ldots,\lambda_4)} \cdot q^{\sum\frac{n(\lambda_i,j)(n(\lambda_i,j)+1)}{2}} \cdot \binom{n}{n(\lambda_i,j),\, n-m(\lambda_1,\ldots,\lambda_4)}_q$$

with $\lambda_1, \ldots, \lambda_4$ being partitions and $m(\lambda_1, \ldots, \lambda_4) = \sum_{i=1}^{4} l(\lambda_i)$. Moreover, $Q(n,k,\gamma)_q$ is a polynomial in q with leading term q^{n^2+n} and

$$\lim_{q\to 1} Q(n,k,\gamma)_q = \binom{n}{k} \cdot (1+\gamma)^{n-k} {}_2F_1^{\mathrm{cl}} \left(\begin{matrix} \frac{k-n}{2} & \frac{k+1-n}{2} \\ & k+1 \end{matrix} \,\middle|\, \frac{4}{(1+\gamma)^2} \right),$$

when $\gamma \neq -1$ and $\lim_{q\to 1} Q(n,k,-1)_q = 0$.

This theorem allows us to determine the Sato–Tate type limiting distribution of the "random part" of matrix point counts on the $K3$ surfaces X_a. More precisely, if n is a positive integer and q is a prime power, then we let

$$A_n(a;q) = N_{n,3}(a;q) - Q(n,0,\phi_q(a+1))_q - R(n,\phi_q(a+1))_q. \tag{1.12}$$

In this notation, we have the following result.

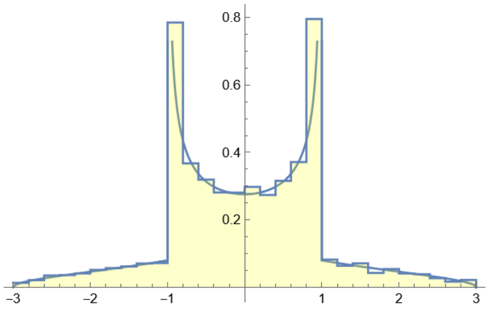
Corollary 1.5. *If $-3 \leq b < c \leq 3$ and n and r are fixed positive integers, then we have*

$$\lim_{p\to\infty} \frac{\{a \in \mathbb{F}_{p^r} : p^{r-rn^2-rn} A_n(a;p^r) \in [b,c]\}}{p^r} = \frac{1}{4\pi} \int_b^c f(t)dt,$$

where

$$f(t) = \begin{cases} \sqrt{\frac{3-|t|}{1+|t|}} & \text{if } 1 < |t| < 3, \\ \sqrt{\frac{3-t}{1+t}} + \sqrt{\frac{3+t}{1-t}} & \text{if } |t| < 1, \\ 0 & \text{otherwise.} \end{cases}$$

Example 1.6. For the prime $p = 93283$, we compare the histogram of the distribution of $p^{-5}A_2(a;p)$ for $a \in \mathbb{F}_p$ with the limiting distribution.



$p^{-5}A_2(a;p)$ histogram for $p = 93283$

This paper is organized as follows. In Section 2 we recall properties of zeta functions for curves and surfaces in the commuting matrix situation. These results [**9**] are due to the first author. In Section 3 we recall results of the second two authors, which we then combine with these zeta functions to obtain our results.

2. Some zeta functions

Let q be a prime power. Recall that $\mathrm{GL}_n(\mathbb{F}_q)$ is the group of $n \times n$ invertible matrices over the finite field $\mathbb{F}_q$ with q elements. It will be repetitively used in this paper that

$$|\mathrm{GL}_n(\mathbb{F}_q)| = (-1)^n q^{\frac{n(n-1)}{2}} (q;q)_n. \tag{2.1}$$

Now, let $X = \operatorname{Spec} R$ be an affine variety over $\mathbb{F}_q$. Say

$$R = \frac{\mathbb{F}_q[T_1, \dots, T_m]}{(f_1, \dots, f_r)}. \tag{2.2}$$

Following the work [**9**] of the first author, we define the set of $n \times n$ *matrix points* on X as the set of commuting tuples of matrices satisfying the defining equations for X:

$$C_n(X) := \left\{ \underline{A} = (A_1, \dots, A_m) \in \operatorname{Mat}_n(\mathbb{F}_q)^m : [A_i, A_j] = 0, f_i(\underline{A}) = 0 \right\}. \tag{2.3}$$

Note that $C_1(X) \cong X(\mathbb{F}_q)$. Though not needed in this paper, it is worth pointing out that the cardinality of $C_n(X)$ is independent of the choice of defining equations for X; in fact, by comparing [**9**, Eq. 4.2] and [**9**, Eq. 4.15], there is an equation-free equivalent characterization for the cardinality of $C_n(X)$:

$$\frac{|C_n(X)|}{|\mathrm{GL}_n(\mathbb{F}_q)|} = \sum_{\dim_{\mathbb{F}_q} H^0(X;M)=n} \frac{1}{|\operatorname{Aut} M|}, \tag{2.4}$$

where the sum ranges over all isomorphism classes of zero-dimensional coherent sheaves on X of degree n. This characterization also makes $|C_n(X)|$ well-defined for any variety X over $\mathbb{F}_q$.

The number of matrix points on a smooth curve or a smooth surface is given by infinite product formulas for a zeta function associated to it. For any (affine) variety X over $\mathbb{F}_q$, consider its *Cohen–Lenstra series* (terminology of [**9**]):

$$\hat{Z}_X(t) := \sum_{n=0}^{\infty} \frac{|C_n(X)|}{|\mathrm{GL}_n(\mathbb{F}_q)|} t^n, \tag{2.5}$$

and recall the local zeta function

$$Z_X(t) := \exp\left(\sum_{n=1}^{\infty} \frac{|X(\mathbb{F}_{q^n})|}{n} t^n \right). \tag{2.6}$$

Proposition 2.1 ([**9**, Proposition 4.6(a)]). *If X is a smooth curve over $\mathbb{F}_q$, then*

$$\hat{Z}_X(t) = \prod_{j \geq 1} Z_X(tq^{-j}). \tag{2.7}$$

Proposition 2.2 ([**9**, Proposition 4.6(b)]). *If X is a smooth surface over $\mathbb{F}_q$, then*

$$\hat{Z}_X(t) = \prod_{i,j \geq 1} Z_X(t^i q^{-j}). \tag{2.8}$$

Proposition 2.1 is essentially due to Cohen and Lenstra [**5**], and Proposition 2.2 is essentially due to the Feit–Fine formula [**6**] for counting commuting matrices and ideas of Bryan and Morrison [**3**]. We remark that both formulas heavily exploit the local geometry of X, namely, smoothness of dimension 1 or 2. In fact, in light of the main theorem of [**9**], Proposition 2.1 ceases to hold if X is a multiplicative reduction of an elliptic curve over a number field (but holds if it is a good reduction).

3. Proofs of Theorems 1.1 and 1.4

Here we use the results of the previous section to prove Theorems 1.1 and 1.4 and their corollaries.

3.1. Proof of Theorem 1.1. Fix a prime power $q = p^r$ with $p \geq 5$ and $r \geq 1$, and fix $a \in \mathbb{F}_q \setminus \{0, 1\}$. Then, denoting by X the affine part of $E_{\mathrm{L}}(a)$, Theorem V.2.4 of [**18**] states that

$$Z_X(t) = \frac{(1 - \alpha t)(1 - \overline{\alpha} t)}{1 - qt},$$

where α and $\overline{\alpha}$ are the traces of Frobenius. Note that there is a missing factor of $\frac{1}{1-t}$ in this expression since we are only considering the affine part of X.

By Proposition 2.1, we then have that

$$\hat{Z}_X(t) = \prod_{j\geq 1} \frac{(1-\alpha t q^{-j})(1-\overline{\alpha} t q^{-j})}{1-tq^{1-j}}.$$

It is well-known due to Euler [**2**, Corollary 2.2] that

$$\prod_{j\geq 1}(1-ctq^{-j}) = \sum_{m\geq 0} \frac{(ct)^m}{(q;q)_m} \tag{3.1}$$

and

$$\prod_{j\geq 1}(1-ctq^{-j})^{-1} = \sum_{m\geq 0} \frac{(-1)^m q^{m(m-1)/2}\cdot (ct)^m}{(q;q)_m}. \tag{3.2}$$

This implies that

$$\hat{Z}_X(t) = \left(\sum_{r\geq 0}\frac{(\alpha t)^r}{(q;q)_r}\right)\cdot\left(\sum_{s\geq 0}\frac{(\overline{\alpha} t)^s}{(q;q)_s}\right)\cdot\left(\sum_{u\geq 0}\frac{(-1)^u q^{u(u+1)/2}\cdot t^u}{(q;q)_u}\right).$$

By the definition of $\hat{Z}_X(t)$ and by (2.1), we then have

$$N_{n,2}(a;q) = (-1)^n q^{n(n-1)/2}(q;q)_n \cdot \sum_{r+s+u=n} \frac{\alpha^r \overline{\alpha}^s (-1)^u q^{\frac{u(u+1)}{2}}}{(q;q)_r (q;q)_s (q;q)_u}.$$

Furthermore, again by Theorem V.2.4 of [**18**], we have that $\alpha\overline{\alpha} = q$ and therefore, we can rewrite this sum as

$$N_{n,2}(a;q) = (-1)^n q^{n(n-1)/2}(q;q)_n \sum_{r+s+u=n} \frac{(-1)^u \alpha^{r-s} q^{s+\frac{u(u+1)}{2}}}{(q;q)_r (q;q)_s (q;q)_u}.$$

Since $a_{\mathrm{L}}(a;q^k) = \alpha^k + \overline{\alpha}^k$, (1.4) implies that

$$N_{n,2}(a;q) = \sum_{k=0}^{n} \phi_{q^k}(-1)\cdot P(n,k)_q \cdot {}_2F_1^{\mathrm{ff}}(a)_{q^k},$$

where

$$P(n,k)_q = (-1)^n q^{\frac{n(n-1)}{2}} (q;q)_n \cdot \sum_{\substack{r-s=k\\ r+s+u=n}} \frac{(-1)^u(-1)^k q^k q^{s+\frac{u(u+1)}{2}}}{(q;q)_r (q;q)_s (q;q)_u}.$$

Rewriting this sum with $r = k+s$ and $u = n-k-2s$, we obtain the expression stated in the theorem.

The leading coefficient of $P(n,k)_q$ is clear from the expression. Since the q-multinomial approaches the usual multinomial as $q\to 1$, we have

$$\lim_{q\to 1} P(n,k)_q = (-1)^k \sum_{s=0}^{\lfloor\frac{n-k}{2}\rfloor} \binom{n}{s, n-k-2s, k+s} = \frac{(-1)^k}{\binom{n}{k}} \sum_{s=0}^{\lfloor\frac{n-k}{2}\rfloor} \frac{k!(n-k)!}{s!(k+s)!(n-k-2s)!}.$$

It is easy to see by induction that if m and s are integers with $m<0$ and $2s+m\leq 0$, then

$$\left(\frac{m}{2}\right)_s \left(\frac{m}{2}+\frac{1}{2}\right)_s = \frac{(-m)!}{(-m-2s)!4^s}.$$

Furthermore, it is evident by definition that for $k\geq 0$, we have $(k+1)_s = \frac{(k+s)!}{k!}$. Applying this above with $m = k-n$, we have

$$\lim_{q\to 1} P(n,k)_q = \frac{(-1)^k}{\binom{n}{k}} \sum_{s=0}^{\lfloor\frac{n-k}{2}\rfloor} \frac{\left(\frac{k-n}{2}\right)_s \left(\frac{k-n+1}{2}\right)_s}{(k+1)_s}\cdot\frac{4^s}{s!},$$

which is our statement since the summand vanishes for $s \geq \lfloor\frac{n-k}{2}\rfloor$.

3.2. Proof of Corollary 1.2. We prove this corollary by implementing the method of moments, as employed in previous work by the second two authors in [**16**]. By Theorem 1.1 and the fact that $p^{\frac{r}{2}}{}_2F_1^{\mathrm{ff}}(a)_{p^r} \in [-2,2]$, we have

$$p^{\frac{r}{2}-rn^2}a_{\mathrm{L},n}(a;p^r) = -\phi_{p^r}(-1)\cdot p^{\frac{r}{2}}{}_2F_1^{\mathrm{ff}}(a)_{p^r} + O_{r,n}(p^{-\frac{r}{2}}).$$

Therefore, if m is a nonnegative integer, we have that

$$\begin{aligned}\frac{1}{p^r}\sum_{a\in\mathbb{F}_{p^r}\setminus\{0,1\}}\left(p^{\frac{r}{2}-rn^2}a_{\mathrm{L},n}(a;p^r)\right)^m &= \frac{1}{p^r}\sum_{a\in\mathbb{F}_{p^r}\setminus\{0,1\}}(-\phi_{p^r}(-1)p^{\frac{r}{2}}{}_2F_1^{\mathrm{ff}}(a)_{p^r})^m \\ &+ \frac{1}{p^r}\sum_{k=1}^{m}\frac{1}{p^{\frac{rk}{2}}}\cdot\binom{m}{k}\frac{1}{p^r}\sum_{a\in\mathbb{F}_{p^r}\setminus\{0,1\}}(-\phi_{p^r}(-1)p^{\frac{r}{2}}{}_2F_1^{\mathrm{ff}}(a)_{p^r})^{m-k} \\ &= \frac{1}{p^r}\sum_{a\in\mathbb{F}_{p^r}\setminus\{0,1\}}(-\phi_{p^r}(-1)p^{\frac{r}{2}}{}_2F_1^{\mathrm{ff}}(a)_{p^r})^m + o_{m,r,n}(1) \text{ as } p\to\infty.\end{aligned}$$

By Theorem 1.1 of [**16**], this implies that as $p \to \infty$ we have

$$\frac{1}{p^r}\sum_{a\in\mathbb{F}_{p^r}\setminus\{0,1\}}\left(p^{\frac{r}{2}-rn^2}a_{\mathrm{L},n}(a;p^r)\right)^m = \begin{cases} o_{m,r,n}(1) & \text{if } m \text{ is odd} \\ \frac{(2l)!}{l!(l+1)!} + o_{m,r,n}(1) & \text{if } m = 2l \text{ is even .}\end{cases}$$

The proof of Corollary 1.2 of [**16**] then implies the limiting distribution.

3.3. Proof of Theorem 1.4. Fix a prime power $q = p^r$ with $p \geq 5$ and $r \geq 1$, and fix $a \in \mathbb{F}_q \setminus \{0,1\}$. Denoting by A_a the affine surface given by

$$s^2 = xy(x+1)(y+1)(x+ay),$$

then $X := A_a$ and X_a differ by a connected union of rational curves (see [**1**, §1]). In particular, we have

$$[X_a] = [X] + 19\mathbb{L} + 1$$

in the Grothendieck ring of $\mathbb{F}_q$-varieties, where $\mathbb{L}$ is the class of the affine line (cf. the terms $(24q-6)-(5q-7)$ at the end of the proof of [**1**, Proposition 4.1]). Therefore, by Theorem 1.1 of [**1**], the local zeta function of X is given by

$$Z_X(t) = \frac{1}{(1-q^2t)(1-\gamma qt)(1-\gamma\alpha^2t)(1-\gamma\overline{\alpha}^2t)},$$

where $\gamma = \phi_q(a+1)$ and $\alpha, \overline{\alpha}$ are the Frobenius eigenvalues for the Clausen elliptic curve $E_{CL}\left(\frac{-1}{a+1}\right)$.

Therefore, by Proposition 2.2, we have that

$$\begin{aligned}\hat{Z}_X(t) &= \prod_{i,j\geq 1}\frac{1}{(1-q^{2-j}t^i)(1-\gamma q^{1-j}t^i)(1-\gamma\alpha^2q^{-j}t^i)(1-\gamma\overline{\alpha}q^{-j}t^i)} \\ &= \prod_{i\geq 1}\prod_{b\in\{q,\gamma,\frac{\gamma\overline{\alpha}^2}{q},\frac{\gamma\alpha^2}{q}\}}\prod_{j\geq 0}\frac{1}{1-bt^iq^{-j}}.\end{aligned}$$

By (3.2) and $\alpha\overline{\alpha} = q$, we then have

$$\begin{aligned}\hat{Z}_X(t) &= \prod_{i\geq 1}\prod_{b\in\{q,\gamma,\frac{\gamma\overline{\alpha}^2}{q},\frac{\gamma\alpha^2}{q}\}}\sum_{m\geq 0}\frac{(-1)^mq^{\frac{m(m+1)}{2}}b^mt^{im}}{(q;q)_m} \\ &= \prod_{i\geq 1}\sum_{m\geq 0}t^{im}\cdot\sum_{m_1+\ldots+m_4=m}\frac{(-1)^mq^{\frac{m_1(m_1+1)}{2}+\ldots+\frac{m_4(m_4+1)}{2}}\gamma^{m_2+m_3+m_4}\cdot q^{m_1-m_3+m_4}\cdot\alpha^{2(m_3-m_4)}}{(q;q)_{m_1}\cdot\ldots\cdot(q;q)_{m_4}} \\ &= \sum_{n\geq 0}t^n\cdot\sum(-1)^{\sum m_{u,v}}\frac{q^{\sum\frac{m_{u,v}(m_{u,v}+1)}{2}}q^{\sum m_{u,1}-m_{u,3}+m_{u,4}}\gamma^{\sum m_{u,2}+m_{u,3}+m_{u,4}}\cdot\pi^{2(\sum m_{u,3}-m_{u,4})}}{\prod(q;q)_{m(u,v)}},\end{aligned}$$

where the latter sum is over all possible combinations of nonnegative integers $m_{u,v}$ with $v = 1, \ldots, 4$ and such that $\sum i_u m_{u,v} = n$ for positive integers $i_u \geq 1$. To simplify this expression, for each $v = 1, \ldots, 4$, we denote by λ_v the partition given by adding i_u with multiplicity $m_{u,v}$.

Then, in the notation of theorem, the coefficient of t^n in $\hat{Z}_X(t)$ is given by

$$\sum_{\substack{\lambda_1,\ldots,\lambda_4 \\ |\lambda_1|+\ldots+|\lambda_4|=n}} (-1)^{l(\lambda_1)+\ldots+l(\lambda_4)} q^{\frac{\sum n(\lambda_i,j)(n(\lambda_i,j)+1)}{2}} q^{l(\lambda_1)-l(\lambda_3)+l(\lambda_4)} \gamma^{l(\lambda_2)+l(\lambda_3)+l(\lambda_4)} \pi^{2(l(\lambda_3)-l(\lambda_4))}.$$

Dividing those partitions into $l(\lambda_3) - l(\lambda_4) = k$ for $0 \leq k \leq n$, using the definition of $\hat{Z}_X(t)$ and using (1.6), we have that

$$N_{n,3}(a;q) = \sum_{k=0}^{n} S(n,k,\phi_q(a+1))_q \left(q^{2k} \cdot \phi_q(a+1)^k \cdot {}_3F_2^{\mathrm{ff}} \left(\frac{a}{a+1} \right)_{q^k} - q^k \right),$$

where

$$S(n,k,\gamma)_q := (-1)^n q^{\frac{n(n-1)}{2}} (q;q)_n \cdot \sum_{\substack{|\lambda_1|+\ldots+|\lambda_4|=n \\ l(\lambda_3)-l(\lambda_4)=k}} (-1)^{m(\lambda_1,\ldots,\lambda_4)} \gamma^{l(\lambda_2)+k+2l(\lambda_4)} \frac{q^{l(\lambda_1)-k} q^{\frac{\sum n(\lambda_i;j)(n(\lambda_i;j)+1)}{2}}}{\prod (q;q)_{m(u,v)}}.$$

The expression for $N_{n,3}(a;q)$ then follows immediately.

The leading coefficient for $Q(n,k,\gamma)_q$ is clear from the definition. It remains to show the behavior of this polynomial as $q \to 1$. To this end, note that $(q;q)_{n-m(\lambda_1,\ldots,\lambda_4)} \to 0$ as $q \to 1$ if $m(\lambda_1, \ldots, \lambda_4) < n$. Therefore, the only contributing partitions are those with $l(\lambda_1) + \ldots + l(\lambda_4) = n$, that is, $\lambda_i = (1, 1, \ldots, 1)$. Therefore, we have

$$\begin{aligned} \lim_{q\to 1} Q(n,k,\gamma)_q &= \sum_{\substack{x+y+z+w=n \\ z-w=k}} \frac{n!}{x!y!z!w!} \cdot \gamma^y \\ &= \sum_{w=0}^{\frac{n-k}{2}} \frac{n!}{w!(w+k)!(n-k-2w)!} \sum_{y=0}^{n-k-2w} \gamma^y \cdot \binom{n-k-2w}{y} \\ &= \sum_{w=0}^{\frac{n-k}{2}} \binom{n}{w, w+k, n-k-2w} (1+y)^{n-k-2w}. \end{aligned}$$

The rest of the proof proceeds exactly as that of Theorem 1.1.

3.4. Proof of Corollary 1.5. We prove this corollary by implementing the method of moments, as employed in previous work by the second two authors in [**16**]. By Theorem 1.4 and the fact that $p^r {}_3F_2^{\mathrm{ff}}(a)_{p^r} \in [-3,3]$, we have

$$p^{r-rn^2-rn} A_n(a;p^r) = p^r {}_3F_2^{\mathrm{ff}}(a)_{p^r} + O_{r,n}(p^{-r}).$$

Therefore, as in the proof of Corollary 1.5, and using Theorem 1.3 of [**16**], for positive integers m, we have that

$$\frac{1}{p^r} \sum_{a\in\mathbb{F}_{p^r}\setminus\{0,1\}} \left(p^{r-rn^2-rn} A_n(a;p^r) \right)^m = \begin{cases} o_{m,r,n}(1) & \text{if } m \text{ is odd} \\ \sum\limits_{i=0}^{m} (-1)^i \binom{m}{i} \frac{(2i)!}{i!(i+1)!} + o_{m,r,n}(1) & \text{if } m \text{ is even.} \end{cases}$$

The proof of Corollary 1.4 of [**16**] then implies the limiting distribution.

References

1. S. Ahlgren, K. Ono, and D. Penniston, *Zeta functions of an infinite family of K3 surfaces*, Amer. J. Math., **124** (2) (2002), 353–368.
2. G. E. Andrews, The theory of partitions, Cambridge Mathematical Library, Cambridge University Press, Cambridge 1998, reprint of the 1976 original.
3. J. Bryan and A. Morrison, *Motivic classes of commuting varieties via power structures*, J. Algebraic Geom. **24(1)** (2015), 183–199

4. T. Clausen, *Über die Fälle, wenn die Reihe von der Form* $y = 1 + \frac{\alpha}{1}, \frac{\beta}{\gamma}x + etc.$ *ein quadrat von der Form* $z = 1 + \frac{\alpha'}{1} \cdot \frac{\beta'}{\gamma'} \cdot \frac{\delta'}{\epsilon'}x + etc.$ *hat*, J. Reine Angew. Math. **3** (1828), 89-91.
5. H. Cohen and H. W. Lenstra Jr., *Heuristics on class groups of number fields*, Lecture Notes in Math. **1068** (1984), Springer, Berlin, 33–62
6. W. Feit and N. J. Fine, *Pairs of commuting matrices over a finite field*, Duke Math. J. **27** (1960), 91–94.
7. J. Greene, *Hypergeometric series over finite fields*, Trans. Amer. Math. Soc. **301** (1987), pages 77-101.
8. J. Greene and D. Stanton, *A character sum evaluation and Gaussian hypergeometric series*, J. Number Theory **23** (1986), 136-148.
9. Y. Huang, *Mutually annihilating matrices, and a Cohen–Lenstra series for the nodal singularity*, J. Alg. **619** (2023), 26–50.
10. D. Husemöller, *Elliptic Curves*, Springer Verlag, Graduate Texts in Mathematics, 111 (2004)
11. M. Ishibashi, H. Sato and K. Shiratani, *On the Hasse invariants of elliptic curves*, Kyushu J. Math.,**48** (1994), no. 2, pages 307-321.
12. M. Koike, *Orthogonal matrices obtained from hypergeometric series over finite fields and elliptic curves over finite fields*, Hiroshima Math. J. **25** (1995), pages 43-52.
13. D. McCarthy, ${}_3F_2$ *hypergeometric series and periods of elliptic curves*, Int. J. Number Theory, **6** (2010), 461-470.
14. K. Ono, *The web of modularity: Arithmetic of the coefficients of modular forms and q-series*, CBMS, Regional Conference series in Mathematics, 102, Amer. Math. Soc., Providence, 2004.
15. K. Ono, *Values of Gaussian hypergeometric series*, Trans. Amer. Math. Soc. **350** (1998), pages 1205-1223.
16. K. Ono, H. Saad, and N. Saikia, *Distribution of values of Gaussian hypergeometric functions*, (https://arxiv.org/abs/2108.09560), Pure and Applied Mathematics Quarterly (Special Issue Celebrating Don Zagier's 70th Birthday), accepted for publication.
17. J. Rouse, *Hypergeometric functions and elliptic curves*, Ramanujan J., **12** (2006), no. 2, pages 197-205.
18. J. Silverman, *The arithmetic of elliptic curves*, Springer Verlag, New York, 1986.

Department of Mathematics, University of British Columbia, Vancouver, BC Canada V6T 1Z2
Email address: huangyf@math.ubc.ca

Department of Mathematics, University of Virginia, Charlottesville, VA 22904
Email address: ken.ono691@virginia.edu

Department of Mathematics, University of Virginia, Charlottesville, VA 22904
Email address: hs7gy@virginia.edu