GAUSSIAN HYPERGEOMETRIC FUNCTIONS AND TRACES OF HECKE OPERATORS

SHARON FRECHETTE, KEN ONO, AND MATTHEW PAPANIKOLAS

ABSTRACT. We establish a simple inductive formula for the trace $\mathrm{Tr}_k^{\mathrm{new}}(\Gamma_0(8), p)$ of the p-th Hecke operator on the space $S_k^{\mathrm{new}}(\Gamma_0(8))$ of newforms of level 8 and weight k in terms of the values of ${}_3F_2$-hypergeometric functions over the finite field $\mathbb{F}_p$. Using this formula when $k = 6$, we prove a conjecture of Koike relating $\mathrm{Tr}_6^{\mathrm{new}}(\Gamma_0(8), p)$ to the values ${}_6F_5(1)_p$ and ${}_4F_3(1)_p$. Furthermore, we find new congruences between $\mathrm{Tr}_k^{\mathrm{new}}(\Gamma_0(8), p)$ and generalized Apéry numbers.

1. Introduction and statement of results

Let p be an odd prime, and let $\mathbb{F}_p$ denote the finite field with p elements. For any multiplicative character χ on $\mathbb{F}_p^\times$, extend χ to a character on $\mathbb{F}_p$ by defining $\chi(0) := 0$. For two characters A and B on $\mathbb{F}_p$, we define the normalized Jacobi sum $\binom{A}{B}$ by

$$\binom{A}{B} := \frac{B(-1)}{p} J(A, \overline{B}) = \frac{1}{p} \sum_{x \in \mathbb{F}_p} A(x)\overline{B}(x-1), \tag{1.1}$$

where $\overline{B}$ is the complex conjugate of the character B.

Let n be a positive integer. For characters $A_0, A_1, \ldots, A_n$ and $B_1, B_2, \ldots, B_n$ on $\mathbb{F}_p$, Greene [9] defined the *Gaussian hypergeometric series over* $\mathbb{F}_p$ by

$$ {}_{n+1}F_n\left(\begin{matrix} A_0, & A_1, & \ldots, & A_n \\ & B_1, & \ldots, & B_n \end{matrix} \middle| x \right)_p := \frac{p}{p-1} \sum_{\chi} \binom{A_0\chi}{\chi} \binom{A_1\chi}{B_1\chi} \cdots \binom{A_n\chi}{B_n\chi} \chi(x), \tag{1.2}$$

where the sum is taken over all characters χ on $\mathbb{F}_p$. Let ε denote the trivial character, and let ϕ denote the quadratic character modulo p (the prime p will always be clear from context). Specializing to our purposes, define

$$ {}_{n+1}F_n(x) := {}_{n+1}F_n\left(\begin{matrix} \phi, & \phi, & \ldots, & \phi \\ & \varepsilon, & \ldots, & \varepsilon \end{matrix} \middle| x \right)_p = \frac{p}{p-1} \sum_{\chi} \binom{\phi\chi}{\chi}^{n+1} \chi(x). \tag{1.3}$$

To emphasize the dependence on p, we will occasionally write ${}_{n+1}F_n(x)_p := {}_{n+1}F_n(x)$.

One important role of Gaussian hypergeometric functions is that they provide formulas for the Fourier coefficients of certain modular forms. For example, if $\lambda \in \mathbb{Q} \setminus \{0, 1\}$ and p is

Date: March 8, 2004; April 27, 2004 (final version).

1991 *Mathematics Subject Classification.* Primary 11F11; Secondary 11F72, 11T24, 33C99.

The first author thanks the Department of Mathematics at Brown University for its hospitality during her visit for the 2002-2003 academic year. The second author is grateful for the support of a grant from the National Science Foundation, and the generous support of the Alfred P. Sloan, David and Lucile Packard, H. I. Romnes, and John S. Guggenheim Fellowships. The third author thanks the support of grants from the NSA MDA904-03-1-0019 and NSF DMS-0340812.

a prime of good reduction for the Legendre normal form elliptic curve

$$E(\lambda): \quad y^2 = x(x-1)(x-\lambda),$$

then $-\phi(-1)p\,{}_2F_1(\lambda)_p$ is the p-th Fourier coefficient of the weight 2 newform associated to $E(\lambda)$ by the Shimura-Taniyama correspondence [12], [17]. Similarly, if

$$\lambda \in \left\{-1, 4, \tfrac{1}{4}, -8, -\tfrac{1}{8}, 64, \tfrac{1}{64}\right\},$$

then, for all but finitely many primes p, it turns out that ${}_3F_2(\lambda)_p$ is essentially the p-th Fourier coefficient of an explicit weight 3 newform with complex multiplication that is associated to a certain singular $K3$ surface X_λ (see Corollary 11.20 of [18]).

In view of these examples, it is natural to seek further formulas for coefficients of modular forms in terms of Gaussian hypergeometric functions. Here we address the problem of obtaining a "Gaussian hypergeometric trace formula" for the action of Hecke operators. For positive integers N and k, let $S_k(\Gamma_0(N))$ denote the space of cusp forms of weight k on the congruence subgroup $\Gamma_0(N)$. Let $S_k^{\text{new}}(\Gamma_0(N))$ denote the subspace generated by its level N newforms. Furthermore, let $\text{Tr}_k(\Gamma_0(N), p)$ denote the trace of the Hecke operator T_p on $S_k(\Gamma_0(N))$, and similarly let $\text{Tr}_k^{\text{new}}(\Gamma_0(N), p)$ denote the trace of T_p on $S_k^{\text{new}}(\Gamma_0(N))$.

The Eichler-Selberg trace formula [10] gives a precise description of $\text{Tr}_k(\Gamma_0(N), p)$; however, the formula is quite complicated (for example, see Theorem 2.2). Here we give a simple formula, inductive in k, for $\text{Tr}_k^{\text{new}}(\Gamma_0(8), p)$ in terms of the values ${}_3F_2(\lambda)$. Moreover, Theorem 1.1 below provides a complete description of the traces of Hecke operators T_p for cusp forms on $\Gamma_0(8)$.

To state this result, we first fix notation. Let $k \geq 2$ be even. If $p \equiv 1 \pmod 4$, then we can uniquely write $p = a^2 + b^2$, where a and b are positive integers, and where a is odd. Then we define

$$\varepsilon_k(p) := \begin{cases} \frac{1}{2}(4a^2 - p)^{\frac{k}{2}-1} + \frac{1}{2}(4b^2 - p)^{\frac{k}{2}-1} & \text{if } p \equiv 1 \pmod 4, \\ -(-p)^{\frac{k}{2}-1} & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{1.4}$$

Remark. Using Theorem 4.3 (2), it is straightforward to verify that

$$\varepsilon_k(p) = \phi(-1)^{\frac{k}{2}} \left[\tfrac{1}{2}(p + p^2\,{}_3F_2(1))^{\frac{k}{2}-1} + \tfrac{1}{2}(p - p^2\,{}_3F_2(1))^{\frac{k}{2}-1}\right]. \tag{1.5}$$

Also, for odd primes p and $k \geq 4$, define the function $H_k(p)$ by

$$H_k(p) := p^{k-2} \sum_{\lambda=2}^{p-1} \phi(-\lambda)\phi(1-\lambda)^{\frac{k}{2}-1}\,{}_3F_2(\lambda)^{\frac{k}{2}-1}, \tag{1.6}$$

and set $H_2(p) := -\phi(-1)$. Let $\left[\begin{smallmatrix} n \\ j \end{smallmatrix}\right]$ denote the trinomial coefficient defined by the expansion

$$(1 + x + x^{-1})^n = \sum_{j=-n}^{n} \left[\begin{array}{c} n \\ j \end{array}\right] x^j. \tag{1.7}$$

Theorem 1.1. *If p is an odd prime and $k \geq 2$ is even, then*

$$\text{Tr}_k^{\text{new}}(\Gamma_0(8), p) = -H_k(p) - \varepsilon_k(p) - \sum_{j=1}^{\frac{k}{2}-1} \left(\left[\begin{array}{c} \frac{k}{2}-1 \\ \frac{k}{2}-j-1 \end{array}\right] - \left[\begin{array}{c} \frac{k}{2}-1 \\ \frac{k}{2}-j \end{array}\right] \right) p^j\, \text{Tr}_{k-2j}^{\text{new}}(\Gamma_0(8), p).$$

Remark. As the referee has kindly pointed out, Theorem 1.1 can also be formulated in terms of generating functions. Moreover, if we let $c_j(d)$ denote the coefficient of x^j in $(1-x)(1+x+x^2)^d$, then Theorem 1.1 becomes the more compact

$$\varepsilon_k(p) + H_k(p) + \sum_{j=0}^{\frac{k}{2}-1} p^j c_j(\tfrac{k}{2}-1)\,\mathrm{Tr}_{k-2j}^{\mathrm{new}}(\Gamma_0(8),p) = 0. \tag{1.8}$$

It is also interesting to consider the generating function $\sum_k \mathrm{Tr}_k^{\mathrm{new}}(\Gamma_0(8),p)x^{\frac{k}{2}-1}$. Using properties of the numbers $c_j(d)$ (see [14, p. 316]), we then find that

$$E(x) + \sum_{\lambda=2}^{p-1} \frac{\phi(-\lambda)}{1-\phi(1-\lambda)p^2\,{}_3F_2(\lambda)x} + A(px) \sum_{k\geq 2 \text{ even}} \mathrm{Tr}_k^{\mathrm{new}}(\Gamma_0(8),p)(xB(px))^{\frac{k}{2}-1} = 0,$$

where

$$A(x) = \frac{1+x-\sqrt{1-2x-3x^2}}{2x(1+x)}, \qquad B(x) = \frac{1-x-\sqrt{1-2x-3x^2}}{2x^2},$$

and

$$E(x) = \begin{cases} \frac{1/2}{1-(4a^2-p)x} + \frac{1/2}{1-(4b^2-p)x} & \text{if } p \equiv 1 \pmod 4, \\ -\frac{1}{1+px} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

By setting

$$R(x) := \frac{x}{1+px+p^2x^2},$$

we then observe

$$\sum_{k\geq 2 \text{ even}} \mathrm{Tr}_k^{\mathrm{new}}(\Gamma_0(8),p)x^{\frac{k}{2}-1} = \tag{1.9}$$

$$-\frac{1+px}{1+px+p^2x^2}\left[E(R(x)) + \sum_{\lambda=2}^{p-1} \frac{\phi(-\lambda)}{1-\phi(1-\lambda)p^2\,{}_3F_2(\lambda)R(x)}\right].$$

Thus $\sum_k \mathrm{Tr}_k^{\mathrm{new}}(\Gamma_0(8),p)x^{\frac{k}{2}-1}$ is a rational function. By computing the values of ${}_3F_2(\lambda)$ explicity, we can compute this rational function for specific values of p. For example, we find

$$\sum_{k\geq 2 \text{ even}} \mathrm{Tr}_k^{\mathrm{new}}(\Gamma_0(8),3)x^{\frac{k}{2}-1} = -\frac{4x}{1+5x+15x^2+27x^3}. \tag{1.10}$$

For larger primes the rational functions become increasingly more complicated.

Remark. It is reasonable to expect that there are generalizations of Theorem 1.1 for other $\Gamma_0(N)$, which will be the subject of further study. However, there does not appear to be a simple way of obtaining a general result in which the choice of parameters in the relevant Gaussian hypergeometric functions are given a priori as a function of N. With the proper hypergeometric functions in hand, it seems likely that proofs of such generalizations would follow from arguments similar to the ones presented here.

Theorem 1.1 has some immediate consequences. Here we describe several applications. As usual, let $\eta(z)$ denote Dedekind's eta-function

$$\eta(z) := q^{1/24}\prod_{n=1}^{\infty}(1-q^n), \tag{1.11}$$

where $q := e^{2\pi iz}$. Let $\eta(2z)^4\eta(4z)^4 = \sum_{n=1}^{\infty} a(n)q^n$ be the unique newform in $S_4^{\text{new}}(\Gamma_0(8))$. If p is an odd prime, then Theorem 1.1 implies that

$$\mathrm{Tr}_4^{\text{new}}(\Gamma_0(8), p) = a(p) = -H_4(p) - \varepsilon_4(p) = -p - p^2 \sum_{\lambda=2}^{p-1} \phi(-\lambda)\phi(1-\lambda)\ {}_3F_2(\lambda).$$

By Theorem 3.13 of [9] (see also Proposition 4.1 (2)), we have $p^2 \sum_{\lambda=2}^{p-1} \phi(-\lambda)\phi(1-\lambda){}_3F_2(\lambda) = p^3\ {}_4F_3(1)$, and so

$$\mathrm{Tr}_4^{\text{new}}(\Gamma_0(8), p) = a(p) = -p^3\ {}_4F_3(1) - p. \tag{1.12}$$

This formula is the conclusion of Theorem 6 of [3], and is equivalent to the assertion that the Calabi-Yau threefold given by

$$x + \frac{1}{x} + y + \frac{1}{y} + z + \frac{1}{z} + w + \frac{1}{w} = 0$$

is modular.

As another application, we recall the following conjecture of Koike [13].

Conjecture (Koike)**.** *Let $\eta(z)^8\eta(4z)^4 + 8\eta(4z)^{12} = \sum_{n=1}^{\infty} b(n)q^n$ be the unique newform in $S_6^{\text{new}}(\Gamma_0(8))$. If p is an odd prime, then*

$$b(p) = -p^5\ {}_6F_5(1) + p^4\ {}_4F_3(1) + (1 - \phi(-1))p^2.$$

By combining Theorem 1.1 with transformation laws for Gaussian hypergeometric functions, we obtain the following.

Corollary 1.2. *Koike's Conjecture is true.*

In addition to their relationship with coefficients of modular forms, Gaussian hypergeometric functions have also played important roles in the proofs of "supercongruence" conjectures of Beukers [5], [6] and Rodriguez-Villegas [20] (see [3], [15], [16]). For primes $p \geq 5$, the following congruence due to Mortenson [16] is typical

$$\sum_{n=0}^{p-1} \frac{(6n)!}{(n!)(2n)!(3n)!} \cdot 2^{-4n}3^{-3n} \equiv \phi(-1) \pmod{p^2}.$$

Other works by Ahlgren [1], Koike [12], and the second author [17] provide further examples of p-adic results for combinatorial expressions whose proofs require these functions.

As an additional application, we consider congruences of the type originally considered by Beukers [5], [6]. If n is a positive integer, then define the *Apéry number* $A(n)$ by

$$A(n) := \sum_{j=0}^{n} \binom{n+j}{j}^2 \binom{n}{j}^2. \tag{1.13}$$

These numbers played an important role in Apéry's celebrated proof of the irrationality of $\zeta(3)$. In 1987, Beukers related these numbers to modular forms [6]; he proved that if p is an odd prime, then

$$\mathrm{Tr}_4^{\text{new}}(\Gamma_0(8), p) \equiv A\left(\frac{p-1}{2}\right) \pmod{p}. \tag{1.14}$$

He went on to conjecture that

$$\mathrm{Tr}_4^{\mathrm{new}}(\Gamma_0(8), p) \equiv A\left(\frac{p-1}{2}\right) \pmod{p^2}.$$

Using (1.12), the Gross-Koblitz formula for the p-adic Gamma-function, some p-adic analysis, and the WZ method, Ahlgren and the second author [3] successfully proved this conjecture.

Using Theorem 1.1, it is now possible to obtain generalizations of such congruences. For brevity, we shall be content with congruences modulo primes p. To state these results, for integers m, ℓ, λ, and n, define the *generalized Apéry number* $A(m, \ell, \lambda; n)$ by

$$A(m, \ell, \lambda; n) := \sum_{j=0}^{n} \binom{n+j}{j}^m \binom{n}{j}^\ell \lambda^j. \tag{1.15}$$

Of course, we have that $A(n) = A(2, 2, 1; n)$.

Theorem 1.3. *Suppose that $k \geq 4$ is even, and that p is an odd prime.*

(1) *If $\frac{k}{2} \equiv 2 \pmod{p-1}$, then*

$$\mathrm{Tr}_k^{\mathrm{new}}(\Gamma_0(8), p) \equiv A\left(\frac{p-1}{2}\right) \pmod{p}.$$

(2) *If $\frac{k}{2} \equiv 3 \pmod{p-1}$, then*

$$\mathrm{Tr}_k^{\mathrm{new}}(\Gamma_0(8), p) \equiv A\left(2, 4, 1; \frac{p-1}{2}\right) \pmod{p}.$$

In general, we have the following.

Theorem 1.4. *If $k \geq 4$ is even and p is an odd prime, then*

$$\mathrm{Tr}_k^{\mathrm{new}}(\Gamma_0(8), p) \equiv -\frac{(1 + (-1)^{\frac{k}{2}-1})}{2} \cdot A\left(1, 2, 1; \frac{p-1}{2}\right)^{\frac{k}{2}-1} - \sum_{\lambda=2}^{p-1} \phi(-\lambda)\phi(1-\lambda)^{\frac{k}{2}-1} A\left(1, 2, \lambda; \frac{p-1}{2}\right)^{\frac{k}{2}-1} \pmod{p}.$$

Remark. Mortenson has kindly pointed out that, as an immediate corollary to Theorem 1.3, one has the following. As in the statement of Koike's conjecture, we let $\sum b(n)q^n$ be the Fourier expansion of the unique newform in $S_6(\Gamma_0(8))$. Then for all odd primes p,

$$b(p) \equiv \sum_{n=0}^{p-1} \frac{(\frac{1}{2})_n^6}{(n!)^6} \pmod{p},$$

where as usual, $(a)_n := a(a+1)\cdots(a+n-1)$ for $n > 0$ and $(a)_0 = 1$. In fact, Mortenson points out that this congruence appears to hold modulo p^5.

In Section 2 we recall a formulation of the Eichler-Selberg trace formula for the groups $\Gamma_0(4)$ and $\Gamma_0(8)$, and we state a formula, which will be proved in Section 7, for the group $\Gamma_0(2)$ (see Theorem 2.3). In Section 3 we then interpret these trace formulas in terms of the numbers of $\mathbb{F}_p$-points on certain classes of varieties, and in Section 4 we recall essential facts regarding Gaussian hypergeometric functions. Assuming the truth of Theorem 2.3, in Section 5 we combine all of these results to prove Theorem 1.1 and Corollary 1.2. In Section 6 we prove Theorems 1.3 and 1.4. In Section 7, we conclude with a proof of Theorem 2.3.

2. Trace formulas

Fix a prime $p \geq 3$, and let $k \geq 2$ be even. Using the version of the Eichler-Selberg trace formula due to Hijikata [10, Thm. 2.2], we will prove formulas for $\mathrm{Tr}_k(\Gamma_0(N), p)$ when $N = 2$, 4, and 8. In the end, we consider simplifications of Hijikata's formula that relate $\mathrm{Tr}_k(\Gamma_0(N), p)$ to the number of points on certain varieties over $\mathbb{F}_p$.

We begin by fixing notation. We will make special use of two families of elliptic curves:

$$ {}_2E_1(\lambda) : y^2 = x(x-1)(x-\lambda), \tag{2.1}$$

$$ {}_3E_2(\lambda) : y^2 = (x-1)(x^2+\lambda). \tag{2.2}$$

For a prime $p \geq 3$ and $\lambda \in \mathbb{F}_p$, the traces of Frobenius ${}_2A_1(p,\lambda)$ and ${}_3A_2(p,\lambda)$ are

$$ {}_2A_1(p,\lambda) = p + 1 - |{}_2E_1(\lambda)(\mathbb{F}_p)|, \quad \lambda \neq 0, 1, \tag{2.3}$$

$$ {}_3A_2(p,\lambda) = p + 1 - |{}_3E_2(\lambda)(\mathbb{F}_p)|, \quad \lambda \neq 0, -1. \tag{2.4}$$

We will rewrite the relevant trace formulas using these quantities.

Let

$$ F_k(x,y) := \frac{x^{k-1} - y^{k-1}}{x - y}. \tag{2.5}$$

The relations $x + y = s$ and $xy = p$ uniquely define a polynomial $G_k(s,p) = F_k(x,y)$. Moreover, a straightforward induction gives

$$ G_k(s,p) = \sum_{j=0}^{\frac{k}{2}-1} (-1)^j \binom{k-2-j}{j} p^j s^{k-2j-2}. \tag{2.6}$$

The polynomial $G_k(s,p)$, evaluated at certain values of s, is a key part of Hijikata's formula for $\mathrm{Tr}_k(\Gamma_0(N), p)$ (e.g. see Theorem 2.2). An important observation is that among the various pieces of Hijikata's formula, for fixed level N, the only part that varies with k is $G_k(s,p)$. Moreover, the points s at which we evaluate $G_k(s,p)$ depend only on p and N and not on k.

The following proposition appears in [2, Thms. 1–2], in the case of level 4, weight 6, and in [4, Thms. 1–2], in the case of level 8, weight 4. In fact, the formulas below hold for all even $k \geq 4$ with exactly the same proofs.

Proposition 2.1 ((1) Ahlgren [2]; (2) Ahlgren-Ono [4]). *If p is an odd prime, and $k \geq 4$ is even, then the following are true.*

(1) $$\mathrm{Tr}_k(\Gamma_0(4), p) = -3 - \sum_{\lambda=2}^{p-1} G_k({}_2A_1(p,\lambda), p).$$

(2) $$\mathrm{Tr}_k(\Gamma_0(8), p) = -4 - \sum_{\lambda=2}^{p-2} G_k({}_2A_1(p,\lambda^2), p).$$

We set more notation. For $d < 0$ and $d \equiv 0$, 1 (mod 4), let $\mathcal{O}(d)$ be the order of discriminant d in the imaginary quadratic field $\mathbb{Q}(\sqrt{d})$. Let $h(\mathcal{O}(d)) = h(d)$ be the class number of $\mathcal{O}(d)$, and $\omega(\mathcal{O}(d)) = \omega(d) = \frac{1}{2}|\mathcal{O}(d)^\times|$. Finally, let $h^*(d) = h(d)/\omega(d)$. Also,

recall the definition of the Kronecker symbol for d,

$$\left(\frac{d}{2}\right) := \begin{cases} 0 & \text{if } d \equiv 0 \pmod 4, \\ 1 & \text{if } d \equiv 1 \pmod 8, \\ -1 & \text{if } d \equiv 5 \pmod 8. \end{cases} \tag{2.7}$$

Theorem 2.2 below is Hijikata's version of the Eichler-Selberg trace formula at level 2, whose derivation from the general formula is a straightforward calculation which we omit.

Theorem 2.2 (Hijikata [10, Thm. 2.2])**.** *Let p be an odd prime, and let $k \geq 2$ be even.*

$$\mathrm{Tr}_k(\Gamma_0(2), p) = -2 - \xi(p)(-p)^{\frac{k}{2}-1} - \sum_{\substack{0<s<2\sqrt{p} \\ s \text{ even}}} G_k(s,p) \sum_{f \mid t} h^*\left(\frac{s^2-4p}{f^2}\right) c(s,f),$$

where

$$\xi(p) = \begin{cases} \frac{1}{2}h^*(-4p) & \text{if } p \equiv 1 \pmod 4, \\ 3h^*(-p) & \text{if } p \equiv 3 \pmod 8, \\ 2h^*(-p) & \text{if } p \equiv 7 \pmod 8, \end{cases}$$

and where if $s^2 - 4p = t^2 D$, with D the discriminant of $\mathbb{Q}(\sqrt{D})$, and if $f \mid t$,

$$c(s,f) = \begin{cases} 1 + \left(\frac{D}{2}\right) & \text{if } \mathrm{ord}_2(f) = \mathrm{ord}_2(t), \\ 2 & \text{if } \mathrm{ord}_2(f) < \mathrm{ord}_2(t). \end{cases}$$

As before, whenever $p \equiv 1 \pmod 4$, we let a, $b \geq 0$, a odd, be defined by the expression $p = a^2 + b^2$. We then define

$$\delta_k(p) := \begin{cases} \frac{1}{2}G_k(2a,p) + \frac{1}{2}G_k(2b,p) & \text{if } p \equiv 1 \pmod 4, \\ (-p)^{\frac{k}{2}-1} & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{2.8}$$

The following theorem provides the level 2 version of Proposition 2.1.

Theorem 2.3. *For a prime $p \geq 3$ and $k \geq 4$ even,*

$$\mathrm{Tr}_k(\Gamma_0(2), p) = -2 - \delta_k(p) - \sum_{\lambda=1}^{p-2} G_k({}_3A_2(p,\lambda), p).$$

We postpone the proof of Theorem 2.3, which is self-contained, until Section 7.

3. Counting points on varieties over $\mathbb{F}_p$

For $k \geq 4$ even, define three sequences of varieties U_k, V_k, and W_k, which are hypersurfaces in affine k-space, by

$$U_k : \ y^2 = \prod_{i=1}^{k-2} (x_i - 1)(x_i^2 + \lambda), \tag{3.1}$$

$$V_k : \ y^2 = \prod_{i=1}^{k-2} x_i(x_i - 1)(x_i - \lambda), \tag{3.2}$$

$$W_k : \ y^2 = \prod_{i=1}^{k-2} x_i(x_i - 1)(x_i - \lambda^2). \tag{3.3}$$

One sees readily that U_k, V_k, and W_k are constructed from families of elliptic curves with subgroups of the form $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$, and $\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ respectively. Geometrically, these varieties are essentially of Kuga-Sato type: for example, there is an easily defined surjective map onto V_k from the $(k-2)$-th power of the Legendre family, fibered over the λ-line. Thus as in Birch [7] and Ihara [11], for a prime $p \geq 3$ it is reasonable to expect that the numbers of points in $U_k(\mathbb{F}_p)$, $V_k(\mathbb{F}_p)$, and $W_k(\mathbb{F}_p)$ are directly related to $\mathrm{Tr}_k(\Gamma_0(2), p)$, $\mathrm{Tr}_k(\Gamma_0(4), p)$, and $\mathrm{Tr}_k(\Gamma_0(8), p)$ respectively. We make these assertions exact in Propositions 3.1, 3.2, and 3.3.

We now consider formulas for $|U_k(\mathbb{F}_p)|$, $|V_k(\mathbb{F}_p)|$, and $|W_k(\mathbb{F}_p)|$ for primes $p \geq 3$. An exact formula for $|W_4(\mathbb{F}_p)|$ was established by Ahlgren and the second author [4, Thm. 1], and one for $|V_6(\mathbb{F}_p)|$ was determined by Ahlgren [2, Thm. 1]. Propositions 3.1–3.3 extend these results to each of $U_k(\mathbb{F}_p)$, $V_k(\mathbb{F}_p)$, $W_k(\mathbb{F}_p)$ for arbitrary even $k \geq 4$.

Let $C(n) = \frac{1}{n+1}\binom{2n}{n}$ be the nth Catalan number, and let $\delta_k(p)$ be as in (2.8).

Proposition 3.1. *For a prime $p \geq 3$ and $k \geq 4$ even,*

$$|U_k(\mathbb{F}_p)| = p^{k-1} + 2 + C\left(\tfrac{k}{2}-1\right)p^{\frac{k}{2}-1}(p+1) - \sum_{j=0}^{\frac{k}{2}-1}\left(\binom{k-2}{j} - \binom{k-2}{j-1}\right)p^j(\mathrm{Tr}_{k-2j}(\Gamma_0(2), p) + \delta_{k-2j}(p) + 2).$$

Remark. It is worth pointing out that the coefficients $\binom{k-2}{j} - \binom{k-2}{j-1}$ are precisely the ones needed to express x^{k-2} in terms of Chebyshev polynomials of the second kind.

Proof. First of all, we have

$$\begin{aligned} |U_k(\mathbb{F}_p)| &= \sum_{\lambda, x_1, \ldots, x_{k-2} \in \mathbb{F}_p} \left\{1 + \phi\left(\prod_{i=1}^{k-2}(x_i - 1)(x_i^2 + \lambda)\right)\right\} \\ &= p^{k-1} + \sum_{\lambda=0}^{p-1}\left\{\sum_{x=0}^{p-1}\phi\Big((x-1)(x^2+\lambda)\Big)\right\}^{k-2} \qquad (3.4) \\ &= p^{k-1} + 2 + \sum_{\lambda=1}^{p-2} {}_3A_2(p, \lambda)^{k-2}. \end{aligned}$$

We will rewrite this expression in terms of the polynomials $G_{k-2j}({}_3A_2(p, \lambda), p)$ for $0 \leq j \leq \frac{k}{2}-1$ using a combinatorial argument involving inverse relations (see Riordan [19, Chs. 2–3]). One such inverse pair [19, Table 2.3] is the following:

$$a_n = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor}\left(\binom{n}{j} - \binom{n}{j-1}\right)b_{n-2j} \quad \text{and} \quad b_n = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor}(-1)^j\binom{n-j}{j}a_{n-2j}. \qquad (3.5)$$

We may rearrange (2.6) to give

$$\frac{G_k(s,p)}{p^{\frac{k}{2}-1}} = \sum_{j=0}^{\frac{k}{2}-1}(-1)^j\binom{k-2-j}{j}\left(\frac{s}{\sqrt{p}}\right)^{k-2-2j}.$$

Setting $n = k-2$, and using $a_n = \left(\frac{s}{\sqrt{p}}\right)^n$ and $b_n = \frac{G_{n+2}(s,p)}{p^{\frac{n}{2}}}$ in (3.5), we obtain

$$s^{k-2} = \sum_{j=0}^{\frac{k}{2}-1} \left(\binom{k-2}{j} - \binom{k-2}{j-1} \right) p^j G_{k-2j}(s,p).$$

Substituting $s = {}_3A_2(p,\lambda)$, the formula in (3.4) therefore becomes

$$\begin{aligned} |U_k(\mathbb{F}_p)| &= p^{k-1} + 2 + \sum_{j=0}^{\frac{k}{2}-1} \left(\binom{k-2}{j} - \binom{k-2}{j-1} \right) p^j \sum_{\lambda=1}^{p-2} G_{k-2j}({}_3A_2(p,\lambda),p) \\ &= p^{k-1} + 2 + \left(\binom{k-2}{\frac{k}{2}-1} - \binom{k-2}{\frac{k}{2}-2} \right) p^{\frac{k}{2}-1}(p-2) \\ &\quad - \sum_{j=0}^{\frac{k}{2}-2} \left(\binom{k-2}{j} - \binom{k-2}{j-1} \right) p^j \Big(\mathrm{Tr}_{k-2j}(\Gamma_0(2),p) + \delta_{k-2j}(p) + 2 \Big), \end{aligned}$$

where for the second equality we apply Theorem 2.3, when $j \leq \frac{k}{2}-2$, and use that $G_2 = 1$, when $j = \frac{k}{2}-1$. Using standard facts about binomial coefficients, we see that

$$\binom{k-2}{\frac{k}{2}-1} - \binom{k-2}{\frac{k}{2}-2} = C\left(\tfrac{k}{2}-1\right).$$

Finally, we adjust the sum to incorporate a $j = \frac{k}{2}-1$ term, which equals $-3C\left(\frac{k}{2}-1\right)p^{\frac{k}{2}-1}$, since $\mathrm{Tr}_2(\Gamma_0(2),p) = 0$ and $\delta_2(p) = 1$, and obtain the desired equality. □

The derivations of the formulas for $|V_k(\mathbb{F}_p)|$ and $|W_k(\mathbb{F}_p)|$ in the following propositions are essentially the same as the proof of Proposition 3.1. The primary differences are that for $|V_k(\mathbb{F}_p)|$ we use Proposition 2.1 (1) instead of Theorem 2.3, and that for $|W_k(\mathbb{F}_p)|$ we use Proposition 2.1 (2). We omit the remaining details.

Proposition 3.2. *For a prime $p \geq 3$ and $k \geq 4$ even,*

$$\begin{aligned} |V_k(\mathbb{F}_p)| = p^{k-1} + 2 + C\left(\tfrac{k}{2}-1\right)p^{\frac{k}{2}-1}(p+1) \\ - \sum_{j=0}^{\frac{k}{2}-1} \left(\binom{k-2}{j} - \binom{k-2}{j-1} \right) p^j \left(\mathrm{Tr}_{k-2j}(\Gamma_0(4),p) + 3 \right). \end{aligned}$$

Proposition 3.3. *For a prime $p \geq 3$ and $k \geq 4$ even,*

$$\begin{aligned} |W_k(\mathbb{F}_p)| = p^{k-1} + 3 + C\left(\tfrac{k}{2}-1\right)p^{\frac{k}{2}-1}(p+1) \\ - \sum_{j=0}^{\frac{k}{2}-1} \left(\binom{k-2}{j} - \binom{k-2}{j-1} \right) p^j \left(\mathrm{Tr}_{k-2j}(\Gamma_0(8),p) + 4 \right). \end{aligned}$$

Combining the numbers of $\mathbb{F}_p$-points on the varieties U_k, V_k, and W_k yields an amusing and useful relationship among the traces $\mathrm{Tr}_k^{\mathrm{new}}(\Gamma_0(8),p)$. Specifically, we put

$$N_k(p) = -|U_k(\mathbb{F}_p)| + 2|V_k(\mathbb{F}_p)| - |W_k(\mathbb{F}_p)|, \tag{3.6}$$

and obtain the following theorem as an immediate consequence of Propositions 3.1–3.3.

Theorem 3.4. *For a prime $p \geq 3$ and $k \geq 4$ even,*

$$N_k(p) = -1 + \sum_{j=0}^{\frac{k}{2}-1} \left(\binom{k-2}{j} - \binom{k-2}{j-1} \right) p^j \left(\mathrm{Tr}^{\mathrm{new}}_{k-2j}(\Gamma_0(8), p) + \delta_{k-2j}(p) \right).$$

4. Gaussian hypergeometric functions

Gaussian hypergeometric functions over finite fields were defined by Greene [9] as character sum analogues of the classical hypergeometric functions. The classical functions satisfy many interesting properties, such as transformation and summation formulas, and Greene showed that their finite field analogues enjoyed many similar properties. Koike [12] and the second author [17] further explored the arithmetic properties of Gaussian hypergeometric functions, including the number-theoretic significance of certain special values of these functions. We continue this study below in Section 5, proving Theorem 1.1 and Koike's conjecture.

In this section, we give several properties of Gaussian hypergeometric functions which we shall require. Using properties of characters and of Jacobi sums, Greene proved an alternate formula for the ${}_2F_1$ function. Also, Greene [9, Thm. 3.13] showed that a Gaussian hypergeometric function can be expressed as a sum of Gaussian hypergeometric functions of lower degree. Specializing these results to the case of ${}_{n+1}F_n(\lambda)$ as defined above, we have the following proposition.

Proposition 4.1 (Greene [9])**.** *If $n \geq 1$ and $\lambda \in \mathbb{F}_p$, then the following hold.*

(1) $${}_2F_1(\lambda) = \frac{\varepsilon(\lambda)\phi(-1)}{p} \sum_{x \in \mathbb{F}_p} \phi(x)\phi(1-x)\phi(1-x\lambda).$$

(2) $${}_{n+1}F_n(\lambda) = \frac{\phi(-1)}{p} \sum_{x \in \mathbb{F}_p} \phi(x)\phi(1-x)\, {}_nF_{n-1}(x\lambda).$$

One of the transformation formulas proved by Greene [9, Thm. 4.2] involves the relationship between a Gaussian hypergeometric series evaluated at λ and at $1/\lambda$. We will have need of two special cases of this theorem, as given in the following proposition.

Proposition 4.2 (Greene [9])**.** *If $\lambda \in \mathbb{F}_p$ is nonzero, then*

(1) ${}_2F_1(\lambda) = \phi(\lambda)\ {}_2F_1(\frac{1}{\lambda})$.

(2) ${}_3F_2(\lambda) = \phi(-\lambda)\ {}_3F_2(\frac{1}{\lambda})$.

We will also have need of the special values ${}_2F_1(-1)$ and ${}_3F_2(1)$. Both parts of the following theorem appear in [17]; part (1) is a special case of Theorem 2, and it is noted that part (2) is a special case of a theorem of Evans.

Theorem 4.3 (Ono [17])**.** *Let p be an odd prime, and if $p \equiv 1 \pmod 4$, then write $p = a^2 + b^2$ where a and b are positive integers, and where a is odd. The following hold.*

(1) $${}_2F_1(-1) = \begin{cases} 0 & \text{if } p \equiv 3 \pmod 4, \\ \dfrac{2a(-1)^{\frac{a+b+1}{2}}}{p} & \text{if } p \equiv 1 \pmod 4. \end{cases}$$

(2) $${}_3F_2(1) = \begin{cases} 0 & \text{if } p \equiv 3 \pmod 4, \\ \dfrac{4a^2 - 2p}{p^2} & \text{if } p \equiv 1 \pmod 4. \end{cases}$$

The following theorem relates the values of ${}_2F_1(\lambda)$ and ${}_3F_2(\lambda)$ to the elliptic curves ${}_2E_1(\lambda)$ and ${}_3E_2(\lambda)$ as defined in Section 2. We note that part (2) is given in [3], as a slight reformulation of [17, Thm. 5].

Theorem 4.4 ((1) Koike [12]; (2) Ono [17])**.** *Let p be an odd prime, and let ${}_2A_1(p,\lambda)$ and ${}_3A_2(p,\lambda)$ be as given in* (2.3) *and* (2.4) *respectively. Then the following are true.*

(1) ${}_2F_1(\lambda) = \dfrac{-\phi(-1)\,{}_2A_1(p,\lambda)}{p}$ *if* $\lambda \neq 0, 1$.

(2) ${}_3F_2\left(1+\dfrac{1}{\lambda}\right) = \dfrac{\phi(-\lambda)\,({}_3A_2(p,\lambda)^2 - p)}{p^2}$ *if* $\lambda \neq 0, -1$.

As a consequence, with certain restrictions on λ, the values ${}_2F_1(\lambda)$ and ${}_3F_2(\lambda)$ are explicitly related to each other.

Corollary 4.5. *If p is an odd prime, then the following hold.*

(1) $p^2\,{}_2F_1(\lambda)^2 = p^2\,{}_3F_2\left(\dfrac{-4\lambda}{(\lambda-1)^2}\right) + p$ *if* $\lambda \neq 0, 1, -1$.

(2) $p^2\,{}_2F_1(-1)^2 = p^2\,{}_3F_2(1) + (1+\phi(-1))p$.

Proof. By Theorem 4.4 (1), if $\lambda \neq 0$, 1, then $p^2\,{}_2F_1(\lambda)^2 = {}_2A_1(p,\lambda)^2$. If $\lambda \neq -1$, then by the change of coordinates $x = \beta x' - \beta$ and $y = \beta^{\frac{3}{2}} y'$, ${}_2E_1(\lambda)$ is isomorphic to the β-quadratic twist of ${}_3E_2(t)$, where $\beta = -\frac{\lambda+1}{2}$ and $t = -\frac{(\lambda-1)^2}{(\lambda+1)^2}$. (See also Lemma 7.1.) It follows that

$$|{}_2E_1(\lambda)(\mathbb{F}_p)| = p + 1 - \phi(\beta)\,{}_3A_2(p,t),$$

hence ${}_2A_1(p,\lambda)^2 = {}_3A_2(p,t)^2$ when $\lambda \neq 0, 1, -1$. Now applying Theorem 4.4 (2) gives $p^2\,{}_2F_1(\lambda)^2 = p^2\,{}_3F_2\big(\frac{-4\lambda}{(\lambda-1)^2}\big) + p$, if $\lambda \neq 0, 1, -1$, since $\phi(-t) = 1$ and $1 + \frac{1}{t} = \frac{-4\lambda}{(\lambda-1)^2}$.

In the case $\lambda = -1$, if $p \equiv 1 \pmod 4$ we write $p = a^2 + b^2$ with a odd. By Theorem 4.3 (1), we have

$$p^2\,{}_2F_1(-1)^2 = \begin{cases} 0 & \text{if } p \equiv 3 \pmod 4, \\ 4a^2 & \text{if } p \equiv 1 \pmod 4. \end{cases}$$

Define $g(\lambda) := p^2\,{}_3F_2\big(\frac{-4\lambda}{(\lambda-1)^2}\big) + p$. By Theorem 4.3 (2), we have

$$g(-1) = \begin{cases} p & \text{if } p \equiv 3 \pmod 4, \\ 4a^2 - p & \text{if } p \equiv 1 \pmod 4, \end{cases}$$

and thus $p^2\,{}_2F_1(-1)^2 = g(-1) + \phi(-1)p = p^2\,{}_3F_2(1) + (1+\phi(-1))p$. □

5. Proofs of Theorem 1.1 and Corollary 1.2

Here we give the proofs of Theorem 1.1 and Corollary 1.2, the latter of which establishes the truth of Koike's conjecture. We require the formula for $|U_k(\mathbb{F}_p)|$ given in (3.4), and the analogous facts about $|V_k(\mathbb{F}_p)|$, and $|W_k(\mathbb{F}_p)|$ as given below. Their derivations are similar

to that of (3.4).

$$|V_k(\mathbb{F}_p)| = p^{k-1} + 2 + \sum_{\lambda=2}^{p-1} {}_2A_1(p,\lambda)^{k-2}, \tag{5.1}$$

$$\begin{aligned} |W_k(\mathbb{F}_p)| &= p^{k-1} + 3 + \sum_{\lambda=2}^{p-1} {}_2A_1(p,\lambda^2)^{k-2} \\ &= p^{k-1} + 3 + \sum_{\lambda=2}^{p-1} (1+\phi(\lambda))\, {}_2A_1(p,\lambda)^{k-2}. \end{aligned} \tag{5.2}$$

Proof of Theorem 1.1. We first note that the case $k = 2$ is trivial, since $\mathrm{Tr}_2^{\mathrm{new}}(\Gamma_0(8), p) = 0$ and $H_2(p) = -\varepsilon_2(p)$. Now fix $k \geq 4$. We require the following expression for $N_k(p)$ in terms of the functions $H_k(p)$, as defined in (3.6) and (1.6) respectively.

Proposition 5.1. *Let p be an odd prime, and let $k \geq 4$ be even. Then*

$$N_k(p) + 1 = -\sum_{j=0}^{\frac{k}{2}-1} \binom{\frac{k}{2}-1}{j} p^j H_{k-2j}(p). \tag{5.3}$$

Proof. By combining (3.4) (with $\lambda \longmapsto \frac{1}{\lambda-1}$), (5.1), and (5.2), and then applying Theorem 4.4, we see that

$$\begin{aligned} N_k(p) + 1 &= -\sum_{\lambda=2}^{p-1} {}_3A_2\left(p, \frac{1}{\lambda-1}\right)^{k-2} + \sum_{\lambda=2}^{p-1} (1-\phi(\lambda))\, {}_2A_1(p,\lambda)^{k-2} \\ &= -\sum_{\lambda=2}^{p-1} \Big(p^2\phi(1-\lambda)\, {}_3F_2(\lambda) + p\Big)^{\frac{k}{2}-1} + \sum_{\lambda=2}^{p-1} (1-\phi(\lambda)) \left(p^2\, {}_2F_1(\lambda)^2\right)^{\frac{k}{2}-1}. \end{aligned}$$

Using Corollary 4.5 on the second sum, we express $N_k(p) + 1$ completely in terms of ${}_3F_2$-functions. Then since $(1-\phi(-1))\big(p^2\, {}_3F_2(1) + (1+\phi(-1))p\big)^{\frac{k}{2}-1} = 0$, we have

$$\begin{aligned} N_k(p) + 1 = -\sum_{\lambda=2}^{p-1} &\Big(p^2\phi(1-\lambda)\, {}_3F_2(\lambda) + p\Big)^{\frac{k}{2}-1} \\ &+ \sum_{\mu=2}^{p-2} (1-\phi(\mu)) \left(p^2\, {}_3F_2\left(\frac{-4\mu}{(\mu-1)^2}\right) + p\right)^{\frac{k}{2}-1}. \end{aligned}$$

To simplify, note that $\frac{-4\mu}{(\mu-1)^2} = \lambda$ if and only if $\mu = \frac{\lambda-2\pm 2\sqrt{1-\lambda}}{\lambda}$. Thus in the second sum, a term containing ${}_3F_2(\lambda)$ appears with multiplicity $1 + \phi(1-\lambda)$. Therefore,

$$\begin{aligned} N_k(p) + 1 = -\sum_{\lambda=2}^{p-1} &\Big(p^2\phi(1-\lambda)\, {}_3F_2(\lambda) + p\Big)^{\frac{k}{2}-1} \\ &+ \sum_{\lambda=2}^{p-1} (1-\phi(-\lambda))(1+\phi(1-\lambda)) \Big(p^2\, {}_3F_2(\lambda) + p\Big)^{\frac{k}{2}-1}. \end{aligned}$$

Expanding the $\big(\frac{k}{2}-1\big)$-th powers using the binomial formula, we then see that (5.3) holds by applying the following lemma. $\square$

Lemma 5.2. *If p is an odd prime, then for any integer $n \geq 0$ the following are true.*

(1) $\displaystyle\sum_{\lambda=2}^{p-1}(1-\phi(-\lambda))\,{}_3F_2(\lambda)^{2n+1} = 0.$

(2) $\displaystyle\sum_{\lambda=2}^{p-1}\phi(1-\lambda)(1-\phi(-\lambda))\,{}_3F_2(\lambda)^{2n} = 0.$

Proof. We prove only part (1). (The proof of part (2) is analogous.) We have

$$\sum_{\lambda=2}^{p-1}(1-\phi(-\lambda))\,{}_3F_2(\lambda)^{2n+1} = \sum_{\lambda=2}^{p-1}{}_3F_2(\lambda)^{2n+1} - \sum_{\lambda=2}^{p-1}\phi(-\lambda)\,{}_3F_2\left(\tfrac{1}{\lambda}\right)^{2n+1},$$

by splitting the sum and taking $\lambda \longmapsto \frac{1}{\lambda}$ in the second piece. Then using Proposition 4.2 (2) on the second piece, we obtain

$$\sum_{\lambda=2}^{p-1}(1-\phi(-\lambda))\,{}_3F_2(\lambda)^{2n+1} = \sum_{\lambda=2}^{p-1}{}_3F_2(\lambda)^{2n+1} - \sum_{\lambda=2}^{p-1}\phi(-\lambda)^{2n+2}\,{}_3F_2(\lambda)^{2n+1} = 0.$$

□

Next we invert the equation from Proposition 5.1, obtaining an expression for $H_k(p)$ in terms of $N_k(p)$ (hence in terms of the trace on spaces of newforms). Recall the definition of $\delta_k(p)$ in (2.8), and let $\gamma_k(p) := -(-p)^{\frac{k}{2}-1}(\phi(-1)-1)$.

Proposition 5.3. *Let p be an odd prime, and let $k \geq 2$ be even. Then*

$$H_k(p) = \gamma_k(p) - \sum_{\ell=0}^{\frac{k}{2}-1}\left(\begin{bmatrix} \frac{k}{2}-1 \\ \frac{k}{2}-\ell-1 \end{bmatrix} - \begin{bmatrix} \frac{k}{2}-1 \\ \frac{k}{2}-\ell \end{bmatrix}\right) p^{\ell}\left(\mathrm{Tr}^{\mathrm{new}}_{k-2\ell}(\Gamma_0(8),p) + \delta_{k-2\ell}(p)\right). \tag{5.4}$$

Proof. Defining $N_2(p) := \phi(-1) - 1$ means that (5.3) holds for all $k \geq 2$. We make use of another inverse pair [19, Table 2.1] given by

$$a_n = \sum_{j=0}^{n}\binom{n}{j} b_{n-j}, \quad \text{and} \quad b_n = \sum_{j=0}^{n}(-1)^j\binom{n}{j} a_{n-j}. \tag{5.5}$$

Dividing through by $p^{\frac{k}{2}}$, (5.3) becomes

$$-\frac{N_k(p)+1}{p^{\frac{k}{2}}} = \sum_{j=0}^{\frac{k}{2}-1}\binom{\frac{k}{2}-1}{j}\frac{H_{k-2j}(p)}{p^{\frac{k}{2}-j}}.$$

Setting $n = \frac{k}{2}-1$, and using $a_n = -\frac{N_{2n+2}(p)+1}{p^{n+1}}$ and $b_n = \frac{H_{2n+2}(p)}{p^{n+1}}$ in (5.5), we obtain

$$H_k(p) = -\sum_{j=0}^{\frac{k}{2}-1}(-1)^j\binom{\frac{k}{2}-1}{j} p^j\left(N_{k-2j}(p)+1\right).$$

Therefore by Theorem 3.4 and our definition of $N_2(p)$, we obtain

$$H_k(p) = \gamma_k(p) - \sum_{j=0}^{\frac{k}{2}-1}(-1)^j \binom{\frac{k}{2}-1}{j} p^j \Bigg\{ \sum_{i=0}^{\frac{k}{2}-1-j} \left(\binom{k-2j-2}{i} - \binom{k-2j-2}{i-1} \right) \times p^i \left(\mathrm{Tr}^{\mathrm{new}}_{k-2(i+j)}(\Gamma_0(8), p) + \delta_{k-2(j+i)}(p) \right) \Bigg\},$$

Now setting $\ell = i + j$ gives

$$H_k(p) = \gamma_k(p) - \sum_{j=0}^{\frac{k}{2}-1}\sum_{\ell=j}^{\frac{k}{2}-1}(-1)^j \binom{\frac{k}{2}-1}{j} \left(\binom{k-2j-2}{\ell-j} - \binom{k-2j-2}{\ell-j-1} \right) \times p^\ell \Big(\mathrm{Tr}^{\mathrm{new}}_{k-2\ell}(\Gamma_0(8), p) + \delta_{k-2\ell}(p) \Big). \tag{5.6}$$

We may adjust the sum on ℓ to range over $0 \le \ell \le \frac{k}{2} - 1$, since the binomial coefficients dependent on ℓ will all be zero if $\ell < j$. We then obtain (5.4) by applying the fact that

$$\left[\begin{array}{c} n \\ m \end{array} \right] = \sum_{j=0}^{n}(-1)^j \binom{n}{j} \binom{2n-2j}{n-m-j}. \tag{5.7}$$

□

The proof of Theorem 1.1 is then complete by applying the following lemma. □

Lemma 5.4. *Let p be an odd prime, and k a positive even integer. Then*

$$\varepsilon_k(p) = -\gamma_k(p) + \sum_{\ell=0}^{\frac{k}{2}-1} \left(\left[\begin{array}{c} \frac{k}{2}-1 \\ \frac{k}{2}-\ell-1 \end{array} \right] - \left[\begin{array}{c} \frac{k}{2}-1 \\ \frac{k}{2}-\ell \end{array} \right] \right) p^\ell \delta_{k-2\ell}(p).$$

Proof. If $p \equiv 3 \pmod 4$, the proof reduces to showing that

$$\sum_{\ell=0}^{\frac{k}{2}-1} \left(\left[\begin{array}{c} \frac{k}{2}-1 \\ \frac{k}{2}-\ell-1 \end{array} \right] - \left[\begin{array}{c} \frac{k}{2}-1 \\ \frac{k}{2}-\ell \end{array} \right] \right) (-1)^\ell = 1.$$

This follows from the easily proven fact that for any $n \ge 0$,

$$\sum_{\ell=0}^{n} \left(\left[\begin{array}{c} n \\ n-\ell \end{array} \right] - \left[\begin{array}{c} n \\ n-\ell+1 \end{array} \right] \right) (-1)^\ell = \sum_{\ell=0}^{2n}(-1)^\ell \left[\begin{array}{c} n \\ n-\ell \end{array} \right].$$

If $p \equiv 1 \pmod 4$, then we must show that

$$\sum_{\ell=0}^{\frac{k}{2}-1} \left(\left[\begin{array}{c} \frac{k}{2}-1 \\ \frac{k}{2}-\ell-1 \end{array} \right] - \left[\begin{array}{c} \frac{k}{2}-1 \\ \frac{k}{2}-\ell \end{array} \right] \right) p^\ell \left(G_{k-2\ell}(2a, p) + G_{k-2\ell}(2b, p) \right) = (4a^2 - p)^{\frac{k}{2}-1} + (4b^2 - p)^{\frac{k}{2}-1}. \tag{5.8}$$

Using the definition of $G_{k-2\ell}(s,p)$, we see that the left-hand side of (5.8) equals

$$\sum_{\ell=0}^{\frac{k}{2}-1}\sum_{i=0}^{\frac{k}{2}-\ell-1}(-1)^i p^{i+\ell}\binom{k-2-i-2\ell}{i} \times\left(\begin{bmatrix}\frac{k}{2}-1\\ \frac{k}{2}-\ell-1\end{bmatrix}-\begin{bmatrix}\frac{k}{2}-1\\ \frac{k}{2}-\ell\end{bmatrix}\right)\left((2a)^{k-2-2(\ell+i)}+(2b)^{k-2-2(\ell+i)}\right).$$

Setting $j=\ell+i$, and noting that $\binom{k-2-j-\ell}{j-\ell}=0$ if $\ell>j$, this expression becomes

$$\sum_{j=0}^{\frac{k}{2}-1}(-1)^j p^j\left\{\sum_{\ell=0}^{\frac{k}{2}-1}(-1)^\ell\binom{k-2-j-\ell}{j-\ell}\left(\begin{bmatrix}\frac{k}{2}-1\\ \frac{k}{2}-\ell-1\end{bmatrix}-\begin{bmatrix}\frac{k}{2}-1\\ \frac{k}{2}-\ell\end{bmatrix}\right)\right\} \times\left((2a)^{k-2-2j}+(2b)^{k-2-2j}\right).$$

Expanding the right-hand-side of (5.8) using the binomial theorem, and comparing it with the above expression, we see that the proof of (5.8) reduces to showing the following equality for every j with $0\le j\le\frac{k}{2}-1$.

$$\binom{\frac{k}{2}-1}{j}=\sum_{\ell=0}^{\frac{k}{2}-1}(-1)^\ell\binom{k-2-j-\ell}{j-\ell}\left(\begin{bmatrix}\frac{k}{2}-1\\ \frac{k}{2}-\ell-1\end{bmatrix}-\begin{bmatrix}\frac{k}{2}-1\\ \frac{k}{2}-\ell\end{bmatrix}\right). \tag{5.9}$$

We prove (5.9) using a third inverse relation. In [19, Table 2.2] (modulo notation), we have the pair

$$\begin{aligned} a_j&=\sum_{\ell=0}^{j}\left(\binom{p+q\ell-\ell}{j-\ell}+q\binom{p+q\ell-\ell}{j-\ell-1}\right)b_\ell,\\ b_j&=\sum_{\ell=0}^{j}(-1)^{\ell+j}\binom{p+qj-\ell}{j-\ell}a_\ell, \end{aligned} \tag{5.10}$$

where p and q are integer parameters. Using (5.7), we may write

$$\begin{bmatrix}n\\ n-j\end{bmatrix}-\begin{bmatrix}n\\ n-j+1\end{bmatrix}=\sum_{\ell=0}^{n}(-1)^\ell\binom{n}{\ell}\left(\binom{2n-2\ell}{j-\ell}-\binom{2n-2\ell}{j-\ell-1}\right).$$

Choosing $p=2n$ and $q=-1$, and noting that $\binom{2n-2\ell}{j-\ell}=0=\binom{2n-2\ell}{j-\ell-1}$ whenever $\ell>j$, we see that this agrees with the first equation in the pair (5.10), with $a_j=\begin{bmatrix}n\\ n-j\end{bmatrix}-\begin{bmatrix}n\\ n-j+1\end{bmatrix}$ and $b_j=(-1)^j\binom{n}{j}$. Inverting the pair then gives

$$(-1)^j\binom{n}{j}=\sum_{\ell=0}^{j}(-1)^{\ell+j}\binom{2n-j-\ell}{j-\ell}\left(\begin{bmatrix}n\\ n-\ell\end{bmatrix}-\begin{bmatrix}n\\ n-\ell+1\end{bmatrix}\right).$$

Setting $n=\frac{k}{2}-1$ and simplifying then gives (5.9). □

We now establish the truth of Koike's Conjecture, using the $k=6$ case of Theorem 1.1.

Proof of Corollary 1.2. Setting $k = 6$ in Theorem 1.1 gives

$$\begin{aligned}\mathrm{Tr}_6^{\mathrm{new}}(\Gamma_0(8), p) &= -H_6(p) - \varepsilon_6(p) - p\,\mathrm{Tr}_4^{\mathrm{new}}(\Gamma_0(8), p)\\ &= -p^4 \sum_{\lambda=1}^{p-1} \phi(-\lambda)\,{}_3F_2(\lambda)^2 + p^4\,{}_4F_3(1) + (1-\phi(-1))p^2,\end{aligned}$$

where in the second equality, we apply (1.5) and (1.12). The proof therefore reduces to establishing the following formula:

$$p^5\,{}_6F_5(1) = p^4 \sum_{\lambda=1}^{p-1} \phi(-\lambda)\,{}_3F_2(\lambda)^2. \tag{5.11}$$

Applying Proposition 4.1 (2) twice to ${}_6F_5(1)$ gives

$$p^5\,{}_6F_5(1) = p^3 \sum_{x=1}^{p-1}\sum_{\lambda=1}^{p-1} \phi(x)\phi(1-x)\phi(\lambda)\phi(1-\lambda)\,{}_4F_3(x\lambda).$$

Applying the change of variables $\lambda \longmapsto \frac{\lambda}{x}$, followed by $x \longmapsto x\lambda$ then yields

$$\begin{aligned}p^5\,{}_6F_5(1) &= p^3 \sum_{\lambda=1}^{p-1} \phi(\lambda)\,{}_4F_3(\lambda) \cdot p\left[\frac{\phi(-1)}{p}\sum_{x=1}^{p-1}\phi(x)\phi(1-x)\phi(1-x\lambda)\right]\\ &= p^4 \sum_{\lambda=1}^{p-1} \phi(\lambda)\,{}_4F_3(\lambda)\,{}_2F_1(\lambda),\end{aligned}$$

where the second equality follows by Proposition 4.1 (1). Now applying Proposition 4.1 (2) to ${}_4F_3(\lambda)$, we see that

$$p^5\,{}_6F_5(1) = \phi(-1)p^3 \sum_{\lambda_1=1}^{p-1}\sum_{\lambda_2=1}^{p-1} \phi(\lambda_1\lambda_2)\phi(1-\lambda_2)\,{}_3F_2(\lambda_1\lambda_2)\,{}_2F_1(\lambda_1).$$

Making the change of variables $\lambda_1\lambda_2 \longmapsto \lambda$ and using the inversion for ${}_2F_1\big(\frac{1}{\lambda_1}\big)$ given in Proposition 4.2 (1), we obtain

$$p^5\,{}_6F_5(1) = \phi(-1)p^3 \sum_{\lambda=1}^{p-1} {}_3F_2(\lambda) \sum_{\lambda_1=1}^{p-1} \phi(\lambda)\phi(\lambda_1-\lambda)\,{}_2F_1\big(\tfrac{1}{\lambda_1}\big).$$

Now putting $\lambda_1 \longmapsto \frac{1}{\lambda_1}$, we see that

$$p^5\,{}_6F_5(1) = \phi(-1)p^3 \sum_{\lambda=1}^{p-1} {}_3F_2(\lambda)\left[\sum_{\lambda_1=1}^{p-1} \phi(\lambda\lambda_1)\phi(1-\lambda\lambda_1)\,{}_2F_1(\lambda_1)\right].$$

By Proposition 4.1, the inner sum equals $\phi(-1)p\,{}_3F_2\big(\frac{1}{\lambda}\big)$. Finally, using the inversion for ${}_3F_2\big(\frac{1}{\lambda_1}\big)$ given in Proposition 4.2, we obtain (5.11), thus completing the proof. □

6. Congruences for $\mathrm{Tr}_k^{\mathrm{new}}(\Gamma_0(8), p)$ modulo p

Here we prove Theorems 1.3 and 1.4 using Theorem 1.1, as well as known facts concerning the values of Gaussian hypergeometric functions modulo p. We state some facts that we require (for example, see [12] or [17, Sect. 5]).

Proposition 6.1. *Suppose that p is an odd prime.*

(1) *If $1 \le \lambda \le p-1$, then*

$$p^2\, {}_3F_2(\lambda) \equiv A\left(1, 2, \lambda; \frac{p-1}{2}\right) \pmod{p}.$$

(2) *We have*

$$p^5\, {}_6F_5(1) \equiv -A\left(2, 4, 1; \frac{p-1}{2}\right) \pmod{p}.$$

Proof of Theorem 1.3. By Theorem 1.1 and the definition of $H_k(p)$ and $\varepsilon_k(p)$, if $\frac{k}{2} \equiv 2 \pmod{p-1}$, then

$$\begin{aligned} \mathrm{Tr}_k^{\mathrm{new}}(\Gamma_0(8), p) &\equiv -H_k(p) - \varepsilon_k(p) \pmod{p} \\ &\equiv -H_4(p) - \varepsilon_4(p) \pmod{p} \\ &= \mathrm{Tr}_4^{\mathrm{new}}(\Gamma_0(8), p). \end{aligned}$$

Theorem 1.3 (1) follows from (1.14).

Similarly, if $\frac{k}{2} \equiv 3 \pmod{p-1}$, then

$$\begin{aligned} \mathrm{Tr}_k^{\mathrm{new}}(\Gamma_0(8), p) &\equiv -H_k(p) - \varepsilon_k(p) \equiv -H_6(p) - \varepsilon_6(p) \pmod{p} \\ &\equiv \mathrm{Tr}_6^{\mathrm{new}}(\Gamma_0(8), p) \pmod{p}. \end{aligned}$$

By Corollary 1.2, it then follows that

$$\mathrm{Tr}_k^{\mathrm{new}}(\Gamma_0(8), p) \equiv -p^5\, {}_6F_5(1) \pmod{p}.$$

Theorem 1.3 (2) now follows immediately from Proposition 6.1 (2). □

Proof of Theorem 1.4. By Theorem 1.1, it follows that

$$\mathrm{Tr}_k^{\mathrm{new}}(\Gamma_0(8), p) \equiv -H_k(p) - \varepsilon_k(p) \pmod{p}.$$

In view of Proposition 6.1 (1), it suffices to show that

$$\varepsilon_k(p) \equiv \frac{(1 + (-1)^{\frac{k}{2}-1})}{2} \cdot \left(p^2\, {}_3F_2(1)\right)^{\frac{k}{2}-1} \pmod{p}. \tag{6.1}$$

Using (1.5), it follows that

$$\varepsilon_k(p) \equiv \tfrac{1}{2}\phi(-1)^{\frac{k}{2}}\left(1 + (-1)^{\frac{k}{2}-1}\right)\left(p^2\, {}_3F_2(1)\right)^{\frac{k}{2}-1} \pmod{p}.$$

If $p \equiv 1 \pmod 4$, this proves (6.1). If $p \equiv 3 \pmod 4$, then $p^2\, {}_3F_2(1) = 0$ by Theorem 4.3 (2). Therefore, (6.1) is also true in these cases. This completes the proof. □

7. The family ${}_3E_2(\lambda)$ and the level 2 trace formula

We devote this section to the proof of Theorem 2.3. The proof follows similar lines to the ones in [2], [4], of the formulas in Proposition 2.1. However, there are several differences which require explanation. Before working out the proof, we go over some facts and lemmas about the family of elliptic curves ${}_3E_2(\lambda) : y^2 = (x-1)(x^2+\lambda)$.

Let K be any field of characteristic $\neq 2$, and consider the family ${}_3E_2(\lambda)$ to be defined over K. Its j-invariant is

$$j({}_3E_2(\lambda)) = \frac{64(3\lambda-1)^3}{\lambda(\lambda+1)^2}.$$

Thus if $j \neq 0$ or 1728, then there are precisely three values of $\lambda \in \overline{K}$ so that $j({}_3E_2(\lambda)) = j$. Moreover, only $j({}_3E_2(\frac{1}{3})) = 0$, and only $j({}_3E_2(-\frac{1}{9})) = j({}_3E_2(\infty)) = 1728$ (so if $\mathrm{char}(K) = 3$, $j({}_3E_2(\lambda))$ is never 0 ($= 1728$) for $\lambda \in K$).

If E/K is an elliptic curve, a *K-quadratic twist* of E is a quadratic twist of E by some $D \in K$.

Lemma 7.1. *Let E/K be an elliptic curve with a K-rational point of order 2 in Weierstrass form $E : y^2 = x^3 + 2\beta x^2 + \gamma x$, with β, $\gamma \in K$ and $\beta \neq 0$. Then there is a $\lambda \in K$ so that E is isomorphic over K to a K-quadratic twist of ${}_3E_2(\lambda)$.*

Proof. The change of coordinates $x = \beta x' - \beta$, $y = \beta^{\frac{3}{2}} y'$, gives the curve ${}_3E_2(\lambda)$, where $\lambda = \frac{\gamma - \beta^2}{\beta^2}$. Thus E is isomorphic over K to the β-quadratic twist of ${}_3E_2(\lambda)$. □

Remark. Lemma 7.1 covers all isomorphism classes of elliptic curves E/K, except when $j(E) = 1728$.

Lemma 7.2. *Suppose that* $\mathrm{char}(K) \neq 3$. *Let $\lambda_1 \in K \setminus \{0, -1, -\frac{1}{9}\}$ and $\lambda_2 \in \overline{K} \setminus \{0, -1\}$. If ${}_3E_2(\lambda_1) \cong {}_3E_2(\lambda_2)$ over $\overline{K}$, then $\lambda_2 \in K(\sqrt{-\lambda_1})$.*

Proof. Any isomorphism ${}_3E_2(\lambda_2) \cong {}_3E_2(\lambda_1)$ over $\overline{K}$ is given by a change of Weierstrass coordinates, $x_1 = u^2 x_2 + r$, $y_1 = u^3 y_2$. Let $\delta^{\pm} = \frac{-1 \pm 3\sqrt{-\lambda_1}}{1+9\lambda_1}$. Then brute force computation yields the following possibilities:

$$\lambda_2 = \lambda_1, \quad u = \pm 1, \quad r = 0;$$
$$\lambda_2 = -\frac{-5 + 3\lambda_1 - 8\delta^{\pm} + 24\lambda_1\delta^{\pm}}{3(1+9\lambda_1)}, \quad u = \pm\sqrt{2\delta^{\pm}}, \quad r = \tfrac{1}{3} - \tfrac{2}{3}\delta^{\pm}.$$

In the second line, there are four possibilities: two choices of $\delta^{\pm}$ and two possible signs on u. In any case, the lemma follows immediately. □

We also appeal to the following theorem of Schoof, specialized to our purposes. For a prime p, let $\mathcal{I}_p$ denote the set of all isomorphism classes of elliptic curves over $\mathbb{F}_p$, and define

$$I(s,p) := \{\mathcal{C} \in \mathcal{I}_p \mid \forall E \in \mathcal{C}, |E(\mathbb{F}_p)| = p + 1 \pm s\}, \tag{7.1}$$

$$I_2(s,p) := \{\mathcal{C} \in I(s,p) \mid \forall E \in \mathcal{C}, E(\mathbb{F}_p)[2] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}\}. \tag{7.2}$$

If $E/\mathbb{F}_p$ is an elliptic curve with $|E(\mathbb{F}_p)| = p + 1 \pm s$, then we write $[E]$ for its class in $I(s,p)$. Also, if $\mathcal{C} \in \mathcal{I}_p$, we let $\mathcal{C}^{\mathrm{tw}} \in \mathcal{I}_p$ be the class of quadratic twists of curves in $\mathcal{C}$ by non-squares

in $\mathbb{F}_p$. If the j-invariant of curves in a class $\mathcal{C}$ is not 1728, then $\mathcal{C} \neq \mathcal{C}^{\mathrm{tw}}$. Also, for d the discriminant of an order $\mathcal{O}$ in an imaginary quadratic field, define the sum of class numbers

$$H(d) := \sum_{\mathcal{O} \subseteq \mathcal{O}' \subseteq \mathcal{O}_{\max}} h(\mathcal{O}'). \tag{7.3}$$

Theorem 7.3 (Schoof [21, (4.5)–(4.9)])**.** *If p is an odd prime, and s is an even integer with $0 \leq s < 2\sqrt{p}$, then*

$$|I(s,p)| = \begin{cases} 2H(s^2-4p) & \text{if } s \neq 0, \\ H(-4p) & \text{if } s = 0. \end{cases}$$

If additionally $s \equiv p+1 \pmod 4$, then

$$|I_2(s,p)| = \begin{cases} 2H\left(\frac{s^2-4p}{4}\right) & \text{if } s \neq 0, \\ h(-p) & \text{if } s = 0. \end{cases}$$

We will need the following lemma on relations between class numbers.

Lemma 7.4 ([8, Cor. 7.28])**.** *Let $\mathcal{O}$ be an order of discriminant d in an imaginary quadratic field, and let $\mathcal{O}' \subseteq \mathcal{O}$ be an order with $[\mathcal{O} : \mathcal{O}'] = f$. Then*

$$h^*(\mathcal{O}') = h^*(\mathcal{O}) \cdot f \prod_{\substack{\ell \mid f \\ \ell \text{ prime}}} \left(1 - \left(\frac{d}{\ell}\right)\frac{1}{\ell}\right).$$

Finally, in the proof of Theorem 2.3 we will make frequent use of the following easily proven lemma.

Lemma 7.5. *Let D be a fundamental discriminant of an imaginary quadratic field. If p is an odd prime and $s^2 - 4p = t^2 D$, then the following hold.*

1. *If $s \equiv p+1 \pmod 4$, then t is even.*
2. *If $s \equiv p-1 \pmod 4$, then t is odd and $D \equiv 0 \pmod 4$.*

Proof of Theorem 2.3. Fix s even with $0 \leq s < 2\sqrt{p}$, and write $s^2 - 4p = t^2 D$ as in the statement of Theorem 2.2. Define

$$L(s,p) := \{\lambda \mid 1 \leq \lambda \leq p-2,\ {}_3A_2(p,\lambda) = \pm s\}. \tag{7.4}$$

We handle the case $p = 3$ first. The only values of s to consider are 0 and 2, and one simply checks that

$$|L(0,3)| = 0 \quad \text{and} \quad |L(2,3)| = 1.$$

It is then a routine matter to check that the $p = 3$ case follows directly from Theorem 2.2. For the remainder of the proof, we will assume that $p \geq 5$.

The elements of $I(s,p)$ can be paired up by quadratic twists so that

$$I(s,p) = \{\mathcal{C}_1, \ldots, \mathcal{C}_h, \mathcal{C}_1^{\mathrm{tw}}, \ldots, \mathcal{C}_h^{\mathrm{tw}}\}.$$

We define

$$\widetilde{I}(s,p) := \{\mathcal{C}_1 \cup \mathcal{C}_1^{\mathrm{tw}}, \ldots, \mathcal{C}_h \cup \mathcal{C}_h^{\mathrm{tw}}\}, \tag{7.5}$$

$$\widetilde{I}_2(s,p) := \{\mathcal{C} \cup \mathcal{C}^{\mathrm{tw}} \mid \mathcal{C} \in I_2(s,p)\}. \tag{7.6}$$

Ultimately we want to relate $|L(s,p)|$, $|\widetilde{I}(s,p)|$, and $|\widetilde{I}_2(s,p)|$. To do this we define

$$\begin{array}{ccc} F : L(s,p) & \longrightarrow & \widetilde{I}(s,p), \\ \lambda & \longmapsto & [{}_3E_2(\lambda)] \cup [{}_3E_2(\lambda)]^{\mathrm{tw}} \end{array} \tag{7.7}$$

and follow with some analysis of its properties.

The case to consider now is when $s \neq 0$. Under this assumption we will show that

$$|L(s,p)| = \sum_{f|t} h^*\left(\frac{s^2-4p}{f^2}\right) c(s,f) - \begin{cases} \frac{1}{2} & \text{if } -\frac{1}{9} \in L(s,p), \\ 0 & \text{otherwise.} \end{cases} \tag{7.8}$$

When $s \neq 0$, we have $-\frac{1}{9} \in L(s,p)$ if and only if $p \equiv 1 \pmod 4$ with $s = 2a$ or $s = 2b$. We can therefore use (7.8) to match up terms in Theorem 2.2 with those in the statement of Theorem 2.3:

$$\begin{aligned} &\sum_{\substack{0<s<2\sqrt{p} \\ s \text{ even}}} G_k(s,p) \sum_{f|t} h^*\left(\frac{s^2-4p}{f^2}\right) c(s,f) \\ &\qquad = \sum_{\lambda=1}^{p-2} G_k({}_3A_2(p,\lambda),p) + \begin{cases} \frac{1}{2}G_k(2a,p) + \frac{1}{2}G_k(2b,p), & \text{if } p \equiv 1 \pmod 4, \\ 0 & \text{if } p \equiv 3 \pmod 4. \end{cases} \end{aligned}$$

The main argument behind (7.8) is contained in the case where $s \neq 0$ and also $\frac{1}{3}$, $-\frac{1}{9} \notin L(s,p)$. We will work out this case first and then consider the remaining details. For s even with $0 < s < 2\sqrt{p}$, we will show that

$$|L(s,p)| = |\widetilde{I}(s,p)| + 2|\widetilde{I}_2(s,p)|. \tag{7.9}$$

Now by Lemma 7.1, the function F is surjective. Since $\frac{1}{3}$, $-\frac{1}{9} \notin L(s,p)$, it follows from Lemma 7.2 that F is 3-to-1 at $\lambda \in L(s,p)$ if and only if $\sqrt{-\lambda} \in \mathbb{F}_p$, which holds if and only if ${}_3E_2(\lambda)(\mathbb{F}_p)[2] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. For all other values of λ, F is 1-to-1. Thus (7.9) holds.

Moreover, if $s \equiv p-1 \pmod 4$, then $|\widetilde{I}_2(s,p)| = 0$ and also, by Lemma 7.5, t is odd and $D \equiv 0 \pmod 4$. Thus

$$|L(s,p)| = |\widetilde{I}(s,p)| = H(s^2-4p) = \sum_{f|t} h^*\left(\frac{s^2-4p}{f^2}\right), \tag{7.10}$$

where the second equality follows from Theorem 7.3 and the third from the assumption that $\frac{1}{3}$, $-\frac{1}{9} \notin L(s,p)$ (so $h\left(\frac{s^2-4p}{f^2}\right) = h^*\left(\frac{s^2-4p}{f^2}\right)$ for all f in consideration). The result then agrees with (7.8). On the other hand, if $s \equiv p+1 \pmod 4$, then t is even by Lemma 7.5, and so by Theorem 7.3,

$$\begin{aligned} |L(s,p)| = |\widetilde{I}(s,p)| + 2|\widetilde{I}_2(s,p)| &= H(s^2-4p) + 2H\left(\frac{s^2-4p}{4}\right) \\ &= \sum_{f|t} h^*\left(\frac{s^2-4p}{f^2}\right) + 2\sum_{f|\frac{t}{2}} h^*\left(\frac{s^2-4p}{4f^2}\right), \end{aligned} \tag{7.11}$$

where the last equality follows because $\frac{1}{3}$, $-\frac{1}{9} \notin L(s,p)$. From Lemma 7.4 it follows that

$$|L(s,p)| = \sum_{f|t} h^*\left(\frac{s^2-4p}{f^2}\right) + \sum_{f|\frac{t}{4}} h^*\left(\frac{s^2-4p}{f^2}\right) + \frac{1}{1-\left(\frac{D}{2}\right)\frac{1}{2}} \cdot \sum_{\substack{f|\frac{t}{2} \\ f\nmid \frac{t}{4}}} h^*\left(\frac{s^2-4p}{f^2}\right). \tag{7.12}$$

Now applying Lemma 7.4 again, we find

$$|L(s,p)| = \left(1+\left(\frac{D}{2}\right)\right) \sum_{\substack{f|t \\ f\nmid \frac{t}{2}}} h^*\left(\frac{s^2-4p}{f^2}\right) + 2\sum_{f|\frac{t}{2}} h^*\left(\frac{s^2-4p}{f^2}\right), \tag{7.13}$$

which verifies (7.8).

The next case to consider is $\frac{1}{3} \in L(s,p)$, where still $s \neq 0$. Then $p \equiv 1 \pmod 3$ and $D = -3$, from which it follows that t is even. Again by Lemma 7.1, F is surjective. Also $-\frac{1}{3} \in \mathbb{F}_p^{\times 2}$, and so $[{}_3E_2(\frac{1}{3})] \cup [{}_3E_2(\frac{1}{3})]^{\mathrm{tw}} \in \widetilde{I}_2(s,p)$. Since F is only 1-to-1 at $\lambda = \frac{1}{3}$ and not 3-to-1, we find

$$|L(s,p)| = |\widetilde{I}(s,p)| + 2|\widetilde{I}_2(s,p)| - 2. \tag{7.14}$$

The argument then follows the same lines as in (7.11)–(7.13), except that when $f = t$, we have $h\left(\frac{s^2-4p}{f^2}\right) = h(-3) = 1 = 3h^*(-3)$. Thus from this fact and from (7.14) we modify (7.11) slightly:

$$|L(s,p)| = -2 + \left[\sum_{f|t} h^*\left(\frac{s^2-4p}{f^2}\right)\right] + \tfrac{2}{3} + \left[2\sum_{f|\frac{t}{2}} h^*\left(\frac{s^2-4p}{4f^2}\right)\right] + \tfrac{4}{3}.$$

Then (7.8) follows precisely as in (7.12) and (7.13).

Now suppose $-\frac{1}{9} \in L(s,p)$, where still $s \neq 0$. Then $p \equiv 1 \pmod 4$ and $D = -4$. There are 4 isomorphism classes of curves over $\mathbb{F}_p$ with j-invariant 1728 [22, Prop. X.5.4], each quartic twists of each other. As elsewhere, write $p = a^2 + b^2$, with a, $b > 0$ and a odd, and then it follows that $s = 2a$ or $s = 2b$. We have

$$[{}_3E_2(-\tfrac{1}{9})] \cup [{}_3E_2(-\tfrac{1}{9})]^{\mathrm{tw}} \in \widetilde{I}(2a,p). \tag{7.15}$$

so if $s = 2a$ the map $F : L(2a,p) \to \widetilde{I}(2a,p)$ is surjective but fails to be 3-to-1 at $-\frac{1}{9}$. Therefore,

$$|L(2a,p)| = |\widetilde{I}(2a,p)| + 2|\widetilde{I}_2(2a,p)| - 2.$$

Since $2b \not\equiv p+1 \pmod 4$, we have $|\widetilde{I}_2(2b,p)| = 0$. Furthermore by (7.15), F misses the class pair of j-invariant 1728 in $\widetilde{I}(2b,p)$, and so

$$|L(2b,p)| = |\widetilde{I}(2b,p)| - 1.$$

Since $h(-4) = 1 = 2h^*(-4)$, we find the present versions of (7.10) and (7.11) to be

$$|L(2a,p)| = -2 + \left[\sum_{f|t} h^*\left(\frac{s^2-4p}{f^2}\right)\right] + \tfrac{1}{2} + \left[2\sum_{f|\frac{t}{2}} h^*\left(\frac{s^2-4p}{4f^2}\right)\right] + 1,$$

$$|L(2b,p)| = -1 + \left[\sum_{f|t} h^*\left(\frac{s^2-4p}{f^2}\right)\right] + \tfrac{1}{2}.$$

The rest of (7.8) follows exactly as in (7.12) and (7.13), which concludes the case $s \neq 0$.

Finally we suppose $s = 0$. We observe that $G_k(0, p) = (-p)^{\frac{k}{2}-1}$, so to conclude the proof of the theorem, we need to verify that

$$|L(0,p)| = \xi(p) - \begin{cases} 0 & \text{if } p \equiv 1 \pmod 4, \\ 1 & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{7.16}$$

The main reason for the discrepancy modulo 4 is that $-\frac{1}{9} \in L(0,p)$ if and only if $p \equiv 3 \pmod 4$. As before we consider the various cases.

If $p \equiv 1 \pmod 4$, then $-\frac{1}{9} \notin L(0,p)$, so by Lemma 7.1, F is surjective. Since $4 \nmid (p+1)$, it follows from Lemma 7.2 that F is 1-to-1,

$$|L(0,p)| = |\widetilde{I}(0,p)| = \tfrac{1}{2}H(-4p) = \tfrac{1}{2}h^*(-4p) = \xi(p),$$

where the second equality follows from Theorem 7.3.

If $p \equiv 3 \pmod 4$, we note that $-\frac{1}{9} \in L(0,p)$. Also $\frac{1}{3} \in L(0,p)$ if and only if $p \equiv 2 \pmod 3$, in which case $-\frac{1}{3} \notin \mathbb{F}_p^{\times 2}$, and so regardless $[{}_3E_2(\frac{1}{3})] \notin I_2(0,p)$. Thus the function F is surjective (Lemma 7.1) but fails to be 3-to-1 at $-\frac{1}{9}$, so as in previous cases,

$$|L(0,p)| = |\widetilde{I}(0,p)| + 2|\widetilde{I}_2(0,p)| - 2.$$

However, now there is a slight difference from the other cases. We note that in fact $[{}_3E_2(-\frac{1}{9})] = [{}_3E_2(-\frac{1}{9})]^{\mathrm{tw}}$ since $p \equiv 3 \pmod 4$ [22, Prop. X.5.4]. Otherwise, for $\mathcal{C} \in I(0,p)$ with $\mathcal{C} \neq [{}_3E_2(-\frac{1}{9})]$, we have $\mathcal{C} \neq \mathcal{C}^{\mathrm{tw}}$. For this reason,

$$|\widetilde{I}_2(0,p)| = \tfrac{1}{2}|I_2(0,p)| + \tfrac{1}{2}.$$

Then combining these equations with Theorem 7.3 and Lemma 7.4,

$$\begin{aligned} |L(0,p)| &= |\widetilde{I}(0,p)| + 2|\widetilde{I}_2(0,p)| - 2 \\ &= \tfrac{1}{2}H(-4p) + h(-p) - 1 \\ &= \tfrac{1}{2}h^*(-4p) + \tfrac{1}{2}h^*(-p) + h^*(-p) - 1 \\ &= \tfrac{3}{2}h^*(-p) + \left\{ \begin{array}{ll} \frac{3}{2} & \text{if } p \equiv 3 \pmod 8 \\ \frac{1}{2} & \text{if } p \equiv 7 \pmod 8 \end{array} \right\} \cdot h^*(-p), \end{aligned}$$

which agrees with (7.16). □

References

[1] S. Ahlgren, *Gaussian hypergeometric series and combinatorial congruences*, Symbolic computation, number theory, special functions, physics and combinatorics (Gainesville, FL, 1999), Kluwer Acad. Publ., Dordrecht, 2001, pp. 1–12.

[2] S. Ahlgren, *The points of a certain fivefold over finite fields and the twelfth power of the eta function*, Finite Fields Appl. **8** (2002), 18–33.

[3] S. Ahlgren and K. Ono, *A Gaussian hypergeometric series evaluation and Apéry number congruences*, J. Reine Angew. Math. **518** (2000), 187–212.

[4] S. Ahlgren and K. Ono, *Modularity of a certain Calabi-Yau threefold*, Monatsh. Math. **129** (2000), 177–190.

[5] F. Beukers, *Some congruences for the Apéry numbers*, J. Number Theory **21** (1985), 141–155.

[6] F. Beukers, *Another congruence for the Apéry numbers*, J. Number Theory **25** (1987), 201–210.

[7] B. J. Birch, *How the number of points of an elliptic curve over a fixed prime field varies*, J. London Math. Soc. **43** (1968), 57–60.

[8] D. A. Cox, *Primes of the form $x^2 + ny^2$*, John Wiley & Sons Inc., New York, 1989.

[9] J. Greene, *Hypergeometric functions over finite fields*, Trans. Amer. Math. Soc. **301** (1987), 77–101.

[10] H. Hijikata, A. K. Pizer, and T. R. Shemanske, *The basis problem for modular forms on* $\Gamma_0(N)$, Mem. Amer. Math. Soc. **82** (1989), vi+159.
[11] Y. Ihara, *Hecke Polynomials as congruence* ζ *functions in elliptic modular case*, Ann. of Math. (2) **85** (1967), 267–295.
[12] M. Koike, *Hypergeometric series over finite fields and Apéry numbers*, Hiroshima Math. J. **22** (1992), 461–467.
[13] M. Koike, private communication.
[14] D. Merlini, D. G. Rogers, R. Sprugnoli, and M. C. Verri, *On some alternative characterizations of Riordan arrays*, Canad. J. Math. **49** (1997), 301–320.
[15] E. Mortenson, *A supercongruence conjecture of Rodriguez-Villegas for a certain truncated hypergeometric function*, J. Number Theory **99** (2003), 139–147.
[16] E. Mortenson, *Supercongruences between* ${}_2F_1$ *hypergeometric functions and their Gaussian analogs*, Trans. Amer. Math. Soc. **355** (2003), 987–1007.
[17] K. Ono, *Values of Gaussian hypergeometric series*, Trans. Amer. Math. Soc. **350** (1998), 1205–1223.
[18] K. Ono, *The web of modularity: arithmetic of the coefficients of modular forms and q-series*, Amer. Math. Soc., Providence, RI, 2004.
[19] J. Riordan, *Combinatorial identities*, John Wiley & Sons Inc., New York, 1968.
[20] F. Rodriguez-Villegas, *Hypergeometric families of Calabi-Yau manifolds*, Calabi-Yau varieties and mirror symmetry (Toronto, ON, 2001), Amer. Math. Soc., Providence, RI, 2003, pp. 223–231.
[21] R. Schoof, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory Ser. A **46** (1987), 183–211.
[22] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.

Department of Mathematics and Computer Science, College of the Holy Cross, Worcester, MA 01610
E-mail address: sfrechet@mathcs.holycross.edu

Department of Mathematics, University of Wisconsin, Madison, WI 53706
E-mail address: ono@math.wisc.edu

Department of Mathematics, Texas A&M University, College Station, TX 77843
E-mail address: map@math.tamu.edu