

## HYPERGEOMETRIC FUNCTIONS OVER $\mathbb{F}_p$ AND RELATIONS TO ELLIPTIC CURVES AND MODULAR FORMS

JENNY G. FUSELIER

(Communicated by Ken Ono)

ABSTRACT. For primes  $p \equiv 1 \pmod{12}$ , we present an explicit relation between the traces of Frobenius on a family of elliptic curves with  $j$ -invariant  $\frac{1728}{t}$  and values of a particular  ${}_2F_1$ -hypergeometric function over  $\mathbb{F}_p$ . We also give a formula for traces of Hecke operators on spaces of cusp forms of weight  $k$  and level 1 in terms of the same traces of Frobenius. This leads to formulas for Ramanujan's  $\tau$ -function in terms of hypergeometric functions.

### 1. INTRODUCTION AND STATEMENT OF MAIN RESULTS

Let  $p$  be a prime and let  $\widehat{\mathbb{F}_p^\times}$  denote the group of all multiplicative characters on  $\mathbb{F}_p^\times$ . We extend  $\chi \in \widehat{\mathbb{F}_p^\times}$  to all of  $\mathbb{F}_p$  by setting  $\chi(0) = 0$ . For  $A, B \in \widehat{\mathbb{F}_p^\times}$ , let  $J(A, B)$  denote the usual Jacobi symbol and define

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

Greene [8] defined *hypergeometric functions over  $\mathbb{F}_p$*  in the following way:

**Definition 1.1** ([8], Defn. 3.10). If  $n$  is a positive integer,  $x \in \mathbb{F}_p$ , and  $A_0, A_1, \dots, A_n, B_1, B_2, \dots, B_n \in \widehat{\mathbb{F}_p^\times}$ , then define

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

Greene explored the properties of these functions and showed that they satisfy many transformations analogous to those enjoyed by their classical counterparts. Recently, Ahlgren, Frechette, Ono, and Papanikolas [1, 2, 3, 6, 14] have proved results linking these hypergeometric functions to modular forms and elliptic curves. The main results given here continue this line of inquiry.

Throughout, we consider a family of elliptic curves having  $j$ -invariant  $\frac{1728}{t}$ . Specifically, for  $t \in \mathbb{F}_p \setminus \{0, 1\}$ , we let

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

---

Received by the editors June 3, 2009.

2000 *Mathematics Subject Classification*. Primary 11F30; Secondary 11T24, 11G20, 33C99.

The author thanks her advisor, Matt Papanikolas, for his advice and support during the preparation of this paper. The author also thanks the Department of Mathematics at Texas A&M University, where the majority of this research was conducted.

Let  $a(t, p)$  denote the trace of the Frobenius endomorphism on  $E_t$ . In particular, for  $t \neq 0, 1$ , we have

$$a(t, p) = p + 1 - \#E_t(\mathbb{F}_p),$$

where  $\#E_t(\mathbb{F}_p)$  counts the number of solutions to  $y^2 \equiv 4x^3 - \frac{27}{1-t}x - \frac{27}{1-t} \pmod{p}$ , including the point at infinity.

Henceforth, we let  $p$  be a prime number with  $p \equiv 1 \pmod{12}$ . We let  $\xi \in \widehat{\mathbb{F}_p^\times}$  have order 12, and we denote by  $\varepsilon$  and  $\phi$  the trivial and quadratic characters, respectively. In this setting, our first main result explicitly relates the above trace of Frobenius and the values of a hypergeometric function over  $\mathbb{F}_p$ .

**Theorem 1.2.** *Suppose  $p \equiv 1 \pmod{12}$  is prime and  $\xi \in \widehat{\mathbb{F}_p^\times}$  has order 12. If  $t \in \mathbb{F}_p \setminus \{0, 1\}$ , then*

$${}_2F_1\left(\xi, \xi^5 \middle| t\right) = \psi(t)a(t, p),$$

where  $\psi(t) = -\phi(2)\xi^{-3}(1-t)$ .

After discussing preliminaries in Section 2, Theorem 1.2 is proved in Section 3. The second main result utilizes the same family of elliptic curves to obtain a trace formula for Hecke operators on spaces of cusp forms of level 1.

Let  $\Gamma = SL_2(\mathbb{Z})$ , and let  $M_k$  and  $S_k$  denote the spaces of modular forms and cusp forms of weight  $k$  for  $\Gamma$ , respectively. Further, let  $\text{Tr}_k(\Gamma, p)$  denote the trace of the Hecke operator  $T_k(p)$  on  $S_k$ . Then the following completely describes these traces  $\text{Tr}_k(\Gamma, p)$ , for a certain class of primes  $p$ .

**Theorem 1.3.** *Suppose  $p \equiv 1 \pmod{12}$  is prime. Let  $a, b \in \mathbb{Z}$  be such that  $p = a^2 + b^2$  and  $a + bi \equiv 1(2 + 2i)$  in  $\mathbb{Z}[i]$ . Also, let  $c, d \in \mathbb{Z}$  be such that  $p = c^2 - cd + d^2$  and  $c + d\omega \equiv 2(3)$  in  $\mathbb{Z}[\omega]$ , where  $\omega = e^{2\pi i/3}$ . Then for even  $k \geq 4$ ,*

$$\text{Tr}_k(\Gamma, p) = -1 - \lambda(k, p) - \sum_{t=2}^{p-1} G_k(a(t, p), p),$$

where

$$\lambda(k, p) = \frac{1}{2}[G_k(2a, p) + G_k(2b, p)] + \frac{1}{3}[G_k(c + d, p) + G_k(2c - d, p) + G_k(c - 2d, p)]$$

and

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

Theorem 1.3 is proved in Section 5. Combining Theorems 1.2 and 1.3 gives a way of writing the traces  $\text{Tr}_k(\Gamma, p)$  in terms of hypergeometric functions. Formulas for Ramanujan's  $\tau$ -function follow by taking  $k = 12$  in Theorem 1.3, and these results are discussed in Section 7.

Finally, Theorem 1.3 gives rise to an inductive formula for the traces  $\text{Tr}_k(\Gamma, p)$  in terms of hypergeometric functions. To state it, we utilize the notation for  $G_k(s, p)$  and  $\lambda(k, p)$  given in Theorem 1.3. We prove this theorem in Section 6.

**Theorem 1.4.** *Suppose  $p \equiv 1 \pmod{12}$  is prime. Let  $k \geq 4$  be even, and define  $m = \frac{k}{2} - 1$ . Then*

$$\begin{aligned} \mathrm{Tr}_{2(m+1)}(\Gamma, p) &= -1 - \lambda(2m+2, p) + b_0(p-2) - \sum_{t=2}^{p-1} p^{2m} \phi^m(1-t) {}_2F_1\left(\xi, \xi^5 \middle| t\right)^{2m} \\ &\quad - \sum_{i=1}^{m-1} b_i(1 + \lambda(2i+2, p)) - \sum_{i=1}^{m-1} b_i \mathrm{Tr}_{2i+2}(\Gamma, p), \end{aligned}$$

where  $b_i = p^{m-i} \left[ \binom{2m}{m-i} - \binom{2m}{m-i-1} \right]$ .

## 2. RELATIONS TO ELLIPTIC CURVES: HISTORY AND PRELIMINARIES

Relationships between hypergeometric functions over  $\mathbb{F}_p$  and elliptic curves are perhaps not surprising since classical hypergeometric series have many known connections to elliptic curves. For example, Beukers [4] gave identifications between periods of families of elliptic curves and values of a particular classical  ${}_2F_1$ -function.

Following Greene's introduction of hypergeometric functions over  $\mathbb{F}_p$ , results emerged linking their values to counting points on varieties over  $\mathbb{F}_p$ . For example, Koike [11] explicitly related the number of points on the Legendre family of elliptic curves over  $\mathbb{F}_p$  to  ${}_2F_1\left(\phi, \phi \middle| t\right)$ , while Ono [13] gave a formula relating the number of points on  $y^2 = (x-1)(x^2+t)$  over  $\mathbb{F}_p$  to a particular  ${}_3F_2$ -function. Later, Ahlgren and Ono [3] related the values of a  ${}_4F_3$ -function to the number of points over  $\mathbb{F}_p$  on a Calabi-Yau 3-fold. Theorem 1.2 is similar in spirit, linking the values of our  ${}_2F_1$ -function to  $\#E_t(\mathbb{F}_p)$ . We now fix notation and recall some basic facts regarding Gauss sums.

Throughout, let  $p \equiv 1 \pmod{12}$  be prime. If  $A \in \widehat{\mathbb{F}_p^\times}$ , let  $G(A) = \sum_{x \in \mathbb{F}_p} A(x) \zeta^x$  denote the Gauss sum, with  $\zeta = e^{2\pi i/p}$ . Since  $\mathbb{F}_p^\times$  is cyclic, let  $T$  denote a fixed generator of the character group and define  $G_m := G(T^m)$ . In particular, recall the following (see [10]):

**Lemma 2.1.**  $G(\varepsilon) = G_0 = -1$  and  $G(\phi) = G_{\frac{p-1}{2}} = \sqrt{p}$  if  $p \equiv 1 \pmod{4}$ .

We now define an additive character  $\theta : \mathbb{F}_p \rightarrow \mathbb{C}$  by  $\theta(\alpha) = \zeta^\alpha$ , and notice that  $G(A) = \sum_{x \in \mathbb{F}_p} A(x) \theta(x)$ . In addition, the following lemma describing  $\theta$  in terms of Gauss sums is straightforward to prove via orthogonality.

**Lemma 2.2.** *Let  $\alpha \in \mathbb{F}_p^\times$ . Then*

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

We also require a few properties of hypergeometric functions over  $\mathbb{F}_p$  from [8]. The first provides a formula for the multiplicative inverse of a Gauss sum, while the second expresses the  ${}_2F_1$ -function as a character sum.

**Lemma 2.3** ([8], Eqn. 1.12). *If  $k \in \mathbb{Z}$  and  $T^k \neq \varepsilon$ , then  $G_k G_{-k} = p T^k(-1)$ .*

**Theorem 2.4** ([8], Defn. 3.5). *If  $A, B, C \in \widehat{\mathbb{F}_p^\times}$  and  $x \in \mathbb{F}_p$ , then*

$${}_2F_1 \left( A, B \middle| C \middle| x \right) = \varepsilon(x) \frac{BC(-1)}{p} \sum_{y=0}^{p-1} B(y) \overline{BC}(1-y) \overline{A}(1-xy).$$

We now give one of Greene's many transformation identities followed by a classical relation on characters. This relation has been rewritten using (1).

**Theorem 2.5** ([8], Theorem 4.4). *If  $A, B, C \in \widehat{\mathbb{F}_p^\times}$  and  $x \in \mathbb{F}_p \setminus \{0, 1\}$ , then*

$${}_2F_1 \left( A, B \middle| C \middle| x \right) = A(-1) {}_2F_1 \left( A, B \middle| ABC \middle| 1-x \right).$$

**Lemma 2.6.** *If  $T^{m-n} \neq \varepsilon$ , then*

$$\begin{pmatrix} T^m \\ T^n \end{pmatrix} = \frac{G_m G_{-n} T^n(-1)}{G_{m-n} \cdot p}.$$

The final character relation we need is the *Hasse-Davenport relation*. We require only two special cases, but the general version can be found in [12].

**Lemma 2.7.** *If  $p \equiv 1 \pmod{4}$  and  $k \in \mathbb{Z}$ , then  $G_{-k} G_{-\frac{p-1}{2}-k} = \sqrt{p} G_{-2k} T^k(4)$ .*

**Lemma 2.8.** *If  $k \in \mathbb{Z}$  and  $p$  is a prime with  $p \equiv 1 \pmod{3}$ , then*

$$G_k G_{k+\frac{p-1}{3}} G_{k+\frac{2(p-1)}{3}} = p T^{-k}(27) T^{\frac{p-1}{3}}(-1) G_{3k}.$$

### 3. PROOF OF THEOREM 1.2

The proof of Theorem 1.2 requires two main steps. First, we derive a formula for  $a(t, p)$  in terms of Gauss sums, and then we do the same for our hypergeometric function. The result follows by comparing the two formulas. Throughout this section, let  $s = \frac{p-1}{12}$  and define  $P(x, y) = y^2 - 4x^3 + \frac{27}{1-t}x + \frac{27}{1-t}$ .

Recall the additive character  $\theta$  defined in the previous section. Note that if  $(x, y) \in \mathbb{F}_p^2$ , then  $\sum_{z \in \mathbb{F}_p} \theta(zP(x, y))$  is  $p$  if  $P(x, y) = 0$  and 0 otherwise. So we have

$$p \cdot (\#E_t(\mathbb{F}_p) - 1) = \sum_{z \in \mathbb{F}_p} \sum_{x, y \in \mathbb{F}_p} \theta(zP(x, y)) = \sum_{x, y \in \mathbb{F}_p} 1 + \sum_{z \in \mathbb{F}_p^\times} \sum_{x, y \in \mathbb{F}_p} \theta(zP(x, y)).$$

Then, by separating the sums according to whether  $x$  and  $y$  are 0 and applying the additivity of  $\theta$ , we have

$$\begin{aligned} p \cdot (\#E_t(\mathbb{F}_p) - 1) &= p^2 + \sum_{z \in \mathbb{F}_p^\times} \theta \left( z \frac{27}{1-t} \right) + \sum_{z \in \mathbb{F}_p^\times} \sum_{y \in \mathbb{F}_p^\times} \theta(zy^2) \theta \left( z \frac{27}{1-t} \right) \\ &\quad + \sum_{z \in \mathbb{F}_p^\times} \sum_{x \in \mathbb{F}_p^\times} \theta(-4zx^3) \theta \left( zx \frac{27}{1-t} \right) \theta \left( z \frac{27}{1-t} \right) \\ &\quad + \sum_{x, y, z \in \mathbb{F}_p^\times} \theta(zP(x, y)) \\ &:= p^2 + A + B + C + D, \end{aligned}$$

where  $A, B, C$ , and  $D$  are set to be the four sums appearing in the previous line. These four sums are computed using the orthogonality relations for characters, and

Lemmas 2.1 and 2.2 repeatedly. We provide the computation for  $C$  here as an example. We begin with three applications of Lemma 2.2 and find that

$$\begin{aligned} C &= \frac{1}{(p-1)^3} \sum_{z \in \mathbb{F}_p^\times} \sum_{x \in \mathbb{F}_p^\times} \sum_{j,k,m=0}^{p-2} G_{-j} G_{-k} G_{-m} T^j(-4zx^3) T^k\left(zx \frac{27}{1-t}\right) T^m\left(z \frac{27}{1-t}\right) \\ &= \frac{1}{(p-1)^3} \sum_{x \in \mathbb{F}_p^\times} \sum_{j,k,m=0}^{p-2} G_{-j} G_{-k} G_{-m} T^j(-4x^3) T^k\left(x \frac{27}{1-t}\right) \\ &\quad \cdot T^m\left(\frac{27}{1-t}\right) \sum_{z \in \mathbb{F}_p^\times} T^{j+k+m}(z), \end{aligned}$$

by collecting all  $T(z)$  terms into a single sum. Note that the final sum is only nonzero when  $m = -j - k$ , by orthogonality. Making this substitution and rearranging gives

$$\begin{aligned} C &= \frac{1}{(p-1)^2} \sum_{j,k=0}^{p-2} G_{-j} G_{-k} G_{j+k} T^j(-4) T^k\left(\frac{27}{1-t}\right) T^{-j-k}\left(\frac{27}{1-t}\right) \sum_{x \in \mathbb{F}_p^\times} T^{3j+k}(x) \\ &= \frac{1}{p-1} \sum_{j=0}^{p-2} G_{-j} G_{3j} G_{-2j} T^j(-4) T^{-j}\left(\frac{27}{1-t}\right). \end{aligned}$$

The last equality follows by substituting  $k = -3j$  and applying orthogonality.

By a similar analysis, one can compute that  $A = -1$ ,  $B = 1 + p\phi\left(\frac{3}{1-t}\right)$ , and

$$D = \frac{1}{p-1} \sum_{k=0}^{p-2} G_{-k} G_{3k} T^k(-4) T^{-k}\left(\frac{27}{1-t}\right) \left[-G_{-2k} + \sqrt{p} G_{6s-2k} \phi\left(\frac{3}{1-t}\right)\right].$$

Combining our calculations for  $A$ ,  $B$ ,  $C$ , and  $D$ , we see that

$$\begin{aligned} p \cdot (\#E_t(\mathbb{F}_p) - 1) &= p^2 + p\phi\left(\frac{3}{1-t}\right) \\ &\quad + \frac{\sqrt{p}}{p-1} \phi\left(\frac{3}{1-t}\right) \sum_{k=0}^{p-2} G_{-k} G_{3k} G_{6s-2k} T^k(-4) T^{-k}\left(\frac{27}{1-t}\right). \end{aligned}$$

Now, since  $a(t, p) = p + 1 - \#E_t(\mathbb{F}_p)$ , we have proved:

**Proposition 3.1.** *If  $p$  is a prime with  $p \equiv 1 \pmod{12}$  and  $s = \frac{p-1}{12}$ , then*

$$a(t, p) = -\phi\left(\frac{3}{1-t}\right) - \frac{\phi\left(\frac{3}{1-t}\right)}{\sqrt{p}(p-1)} \sum_{k=0}^{p-2} G_{-k} G_{3k} G_{6s-2k} T^k(-4) T^{-k}\left(\frac{27}{1-t}\right).$$

Now that we have a formula for the trace of Frobenius on  $E_t$  in terms of Gauss sums, we write our  ${}_2F_1$ -function in similar terms. Note that in Theorem 1.2 we may take the character  $\xi$  to be  $T^s$ .

**Proposition 3.2.** *For  $t \in \mathbb{F}_p \setminus \{0, 1\}$ ,*

$${}_2F_1\left(\xi, \xi^5 \middle| t\right) = \frac{T^{3s}(4(1-t))}{\sqrt{p}(p-1)} \sum_{k=0}^{p-2} G_{6s-2k} G_{3k} \frac{1}{G_k} T^k(4) T^{-k}\left(\frac{27}{1-t}\right).$$

*Proof.* Beginning with Theorem 2.5 and Definition 1.1,

$${}_2F_1\left(\xi, \xi^5 \middle| t\right) = T^s(-1) \frac{p}{p-1} \sum_{k=0}^{p-2} \binom{T^{s+k}}{T^k} \binom{T^{5s+k}}{T^{6s+k}} T^k (1-t),$$

since  $T$  generates  $\widehat{\mathbb{F}}_p^\times$ . Now we rewrite the product  $\binom{T^{s+k}}{T^k} \binom{T^{5s+k}}{T^{6s+k}}$  in terms of Gauss sums, via Lemma 2.6. As  $T^s = \xi$  and  $T^{-s} = \xi^{-1}$  are not trivial, we have

$$\binom{T^{s+k}}{T^k} \binom{T^{5s+k}}{T^{6s+k}} = \frac{1}{p^3} G_{s+k} G_{-k} G_{5s+k} G_{-6s-k} T^{5s+2k}(-1),$$

since  $G_s G_{-s} = pT^s(-1)$  by Lemma 2.3. Combining with our initial calculation,

$${}_2F_1\left(\xi, \xi^5 \middle| t\right) = \frac{\phi(-1)}{p^2(p-1)} \sum_{k=0}^{p-2} G_{s+k} G_{-k} G_{5s+k} G_{-6s-k} T^k (1-t),$$

because  $T^s T^{5s} = \phi$  and  $T^{2k}(-1) = 1$  for all  $k$ .

Now we apply Lemma 2.7 and make a substitution for  $G_{-k} G_{-6s-k}$ . We obtain

$${}_2F_1\left(\xi, \xi^5 \middle| t\right) = \frac{\phi(-1)}{p^{\frac{3}{2}}(p-1)} \sum_{k=0}^{p-2} G_{s+k} G_{5s+k} G_{-2k} T^k(4) T^k (1-t).$$

Next, we let  $k \mapsto k + 3s$  and find

$$\begin{aligned} {}_2F_1\left(\xi, \xi^5 \middle| t\right) &= \frac{\phi(-1)}{p^{\frac{3}{2}}(p-1)} \sum_{k=0}^{p-2} G_{4s+k} G_{8s+k} G_{-2k-6s} T^{k+3s}(4) T^{k+3s} (1-t) \\ &= \frac{\phi(-1) T^{4s}(-1)}{\sqrt{p}(p-1)} \sum_{k=0}^{p-2} G_{6s-2k} G_{3k} \frac{1}{G_k} T^{-k}(27) T^{k+3s}(4) T^{k+3s} (1-t), \end{aligned}$$

by applying Lemma 2.8 to make a substitution for  $G_{4s+k} G_{8s+k}$ , and by noting that  $G_{-2k-6s} = G_{-2k+6s}$ . Then, since  $p \equiv 1 \pmod{12}$  implies  $\phi(-1) T^{4s}(-1) = T^{10s}(-1) = 1$ , the result follows.  $\square$

We now have the necessary tools to complete the proof of Theorem 1.2.

*Proof of Theorem 1.2.* By Lemma 2.3, Proposition 3.2, and the fact that  $T^{-k}(-1) = T^k(-1)$  implies  $T^{-k}(-1) T^k(4) = T^k(-4)$ , we have

$${}_2F_1\left(\xi, \xi^5 \middle| t\right) = \frac{T^{3s}(4(1-t))}{\sqrt{p}(p-1)} \left[ \sqrt{p} + \frac{1}{p} \sum_{k=1}^{p-2} G_{6s-2k} G_{3k} G_{-k} T^k(-4) T^{-k} \left( \frac{27}{1-t} \right) \right].$$

Next, we multiply by  $\frac{\phi(3)T^{3s}(1-t)}{\phi(3)T^{3s}(1-t)}$  and rearrange, recalling  $\phi = \phi^{-1}$ . We obtain

(3)

$$\begin{aligned} {}_2F_1\left(\xi, \xi^5 \middle| t\right) &= -\frac{T^{3s}(4)}{\phi(3)T^{3s}(1-t)} \left[ -\frac{1}{p-1} \phi\left(\frac{3}{1-t}\right) \right. \\ &\quad \left. - \frac{1}{p^{\frac{3}{2}}(p-1)} \phi\left(\frac{3}{1-t}\right) \sum_{k=1}^{p-2} G_{6s-2k} G_{3k} G_{-k} T^k (-4) T^{-k} \left(\frac{27}{1-t}\right) \right] \\ &= -T^{3s}(4) \phi(3) T^{-3s}(1-t) \left[ -\frac{\phi\left(\frac{3}{1-t}\right)}{p} \right. \\ &\quad \left. - \frac{\phi\left(\frac{3}{1-t}\right)}{p^{\frac{3}{2}}(p-1)} \sum_{k=0}^{p-2} G_{6s-2k} G_{3k} G_{-k} T^k (-4) T^{-k} \left(\frac{27}{1-t}\right) \right]. \end{aligned}$$

The last equality follows since the  $k = 0$  term of the final sum is  $-\frac{\phi\left(\frac{3}{1-t}\right)}{p(p-1)}$ . By Proposition 3.1 and (3), we have that

$$p {}_2F_1\left(\xi, \xi^5 \middle| t\right) = -T^{3s}(4) \phi(3) T^{-3s}(1-t) a(t, p),$$

so the proof is complete if  $T^{3s}(4) \phi(3) T^{-3s}(1-t) = \phi(2) \xi^{-3}(1-t)$ . Since  $T^{3s} = \xi^3$  and  $T^{-3s} = \xi^{-3}$ , we need only show that  $\xi^3(4) \phi(3) = \phi(2)$ . By multiplicativity,  $\xi^3(4) = \xi^6(2) = \phi(2)$ . Further,  $\phi(3) = \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$  by quadratic reciprocity, since  $p \equiv 1 \pmod{4}$ . Since  $p \equiv 1 \pmod{3}$ ,  $\phi(3) = \left(\frac{1}{3}\right) = 1$ , completing the proof.  $\square$

#### 4. RELATIONS TO MODULAR FORMS: HISTORY AND PRELIMINARIES

As with elliptic curves, classical hypergeometric functions have well-known connections to modular forms. We were motivated by work of Stiller [18], on connections among classical hypergeometric series, families of elliptic curves, and modular forms, to choose the family  $E_t$  and the  ${}_2F_1$ -function in our main results.

Following Greene's introduction of hypergeometric functions over finite fields, results emerged relating them to modular forms. Ahlgren, Ono, Frechette, and Papanikolas [1, 2, 6] produced formulas for traces of Hecke operators on certain spaces of cusp forms. These were given in terms of counting points on related varieties over finite fields. Papanikolas [14] used these to obtain a formula for Ramanujan's  $\tau$ -function as well as a congruence for  $\tau(p)$  modulo 11.

Let  $k \geq 2$  be an even integer, and define  $F_k(x, y) = \frac{x^{k-1} - y^{k-1}}{x - y}$ . Then letting  $x + y = s$  and  $xy = p$  gives rise to polynomials  $G_k(s, p) = F_k(x, y)$ . These polynomials can be written alternatively as

$$(4) \quad G_k(s, p) = \sum_{j=0}^{\frac{k}{2}-1} (-1)^j \binom{k-2-j}{j} p^j s^{k-2j-2}.$$

In the proof of Theorem 1.3 we work with traces of Hecke operators on spaces of cusp forms of level 1. We apply similar techniques to those used by Ahlgren and Ono [2] for level 8, Ahlgren [1] for level 4, and Frechette, Ono, and Papanikolas [6] for level 2. First, we use Hasse's classical bound on the number of points on

an elliptic curve defined over a finite field [17]. We also use a theorem of Schoof together with Hijikata's version of the Eichler-Selberg trace formula, which require some notation. We follow the treatment given in [6]. If  $d < 0$ ,  $d \equiv 0, 1 \pmod{4}$ , let  $\mathcal{O}(d)$  denote the unique imaginary quadratic order in  $\mathbb{Q}(\sqrt{d})$  having discriminant  $d$ . Let  $h(d) = h(\mathcal{O}(d))$  be the order of the class group of  $\mathcal{O}(d)$ , and let  $w(d) = w(\mathcal{O}(d))$  be half the cardinality of the unit group of  $\mathcal{O}(d)$ . We then let  $h^*(d) = h(d)/w(d)$ . Further, if  $d$  is the discriminant of an imaginary quadratic order  $\mathcal{O}$ , let

$$(5) \quad H(d) := \sum_{\mathcal{O}' \subseteq \mathcal{O} \subseteq \mathcal{O}_{\max}} h(\mathcal{O}'),$$

where the sum is over all orders  $\mathcal{O}'$  between  $\mathcal{O}$  and the maximal order  $\mathcal{O}_{\max}$ . A complete treatment of the theory of orders in imaginary quadratic fields can be found in section 7 of [5].

Additionally, if  $K$  is a perfect field, we define  $Ell_K := \{[E]_K : E \text{ is defined over } K\}$ , where  $[E]_K$  denotes the isomorphism class of  $E$  over  $K$  and  $[E_1]_K = [E_2]_K$  if there exists an isomorphism  $\beta : E_1 \rightarrow E_2$  over  $K$ . Now if  $p$  is an odd prime, define

$$(6) \quad I(s, p) := \{[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p} : \#E(\mathbb{F}_p) = p + 1 \pm s\}.$$

Schoof proved the following theorem which connects (5) and (6).

**Theorem 4.1** ([16], Thm. 4.6). *If  $p$  is an odd prime and  $s$  is an integer with  $0 < s < 2\sqrt{p}$ , then  $\#I(s, p) = 2H(s^2 - 4p)$ .*

The final key ingredient to the proof of Theorem 1.3 is the Eichler-Selberg trace formula, which provides a starting point for calculating  $\text{Tr}_k(\Gamma, p)$ . We use Hijikata's version of this formula [9] and state the level 1 formulation in terms of the polynomials  $G_k(s, p)$ .

**Theorem 4.2** ([9], Thm. 2.2). *Let  $k \geq 2$  be an even integer, and let  $p \equiv 1 \pmod{12}$  be prime. Then*

$$\text{Tr}_k(\Gamma, p) = -h^*(-4p)(-p)^{\frac{k}{2}-1} - 1 - \sum_{0 < s < 2\sqrt{p}} G_k(s, p) \sum_{f|\ell} h^*\left(\frac{s^2 - 4p}{f^2}\right) + \delta(k),$$

where  $\delta(k) = p + 1$  if  $k = 2$  and 0 otherwise, and where we classify integers  $s$  with  $s^2 - 4p < 0$  by some positive integer  $\ell$  and square-free integer  $m$  via

$$s^2 - 4p = \begin{cases} \ell^2 m, & 0 > m \equiv 1 \pmod{4}, \\ \ell^2 4m, & 0 > m \equiv 2, 3 \pmod{4}. \end{cases}$$

We end this section by recalling the following result on elliptic curves. The proof may be found in Section X.5 of [17].

**Lemma 4.3.** *Let  $p \geq 5$  be prime, and define  $\eta : Ell_{\mathbb{F}_p} \rightarrow Ell_{\mathbb{F}_p}$  by  $[E]_{\mathbb{F}_p} \mapsto [E]_{\mathbb{F}_p}$ . If  $[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p}$  and  $E$  is defined over  $\mathbb{F}_p$ . Then*

$$\#\eta^{-1}([E]_{\mathbb{F}_p}) = \begin{cases} 2 & \text{if } j \neq 0, 1728, \\ 4 & \text{if } j = 1728, \\ 6 & \text{if } j = 0. \end{cases}$$

5. PROOF OF THEOREM 1.3

Among isomorphism classes of elliptic curves over  $\mathbb{F}_p$ , we begin with those having  $j$ -invariant 1728 or 0. If  $E$  is any elliptic curve defined over  $\mathbb{F}_p$ , we let  $a(E)$  be given by  $a(E) = p + 1 - \#E(\mathbb{F}_p)$ . The following two lemmas compute formulas for the sums of  $a(E)^n$  over all such curves.

**Lemma 5.1** ([7], Lemma IV.3.3). *Let  $p \equiv 1 \pmod{12}$  and let  $a, b \in \mathbb{Z}$  be such that  $p = a^2 + b^2$  and  $a + bi \equiv 1 \pmod{2 + 2i}$  in  $\mathbb{Z}[i]$ . Then for  $n \geq 2$  even,*

$$\sum_{\substack{[E]_{\mathbb{F}_p} \in \text{Ell}_{\mathbb{F}_p} \\ j(E)=1728}} a(E)^n = 2^{n+1}(a^n + b^n).$$

**Lemma 5.2** ([7], Lemma IV.3.5). *Let  $p \equiv 1 \pmod{12}$  and let  $c, d \in \mathbb{Z}$  be such that  $p = c^2 - cd + d^2$  and  $c + d\omega \equiv 2 \pmod{3}$  in  $\mathbb{Z}[\omega]$ , where  $\omega = e^{2\pi i/3}$ . Then for  $n \geq 2$  even,*

$$\sum_{\substack{[E]_{\mathbb{F}_p} \in \text{Ell}_{\mathbb{F}_p} \\ j(E)=0}} a(E)^n = 2[(c + d)^n + (2c - d)^n + (c - 2d)^n].$$

We omit the proofs of Lemmas 5.1 and 5.2. They are not difficult, but require checking dozens of cases. Complete details can be found in [7]. Now we proceed toward the proof of Theorem 1.3, beginning with a lemma relating  $h$  to  $h^*$ . In the following two results, we classify integers  $s$  with  $s^2 - 4p < 0$  by some positive integer  $\ell$  and square-free integer  $m$  via

$$(7) \quad s^2 - 4p = \begin{cases} \ell^2 m, & 0 > m \equiv 1 \pmod{4}, \\ \ell^2 4m, & 0 > m \equiv 2, 3 \pmod{4}. \end{cases}$$

**Lemma 5.3.** *If  $p \equiv 1 \pmod{12}$  is prime, then for  $n \geq 2$  even,*

$$\begin{aligned} \sum_{0 < s < 2\sqrt{p}} s^n \sum_{f|\ell} h\left(\frac{s^2 - 4p}{f^2}\right) &= \sum_{0 < s < 2\sqrt{p}} s^n \sum_{f|\ell} h^*\left(\frac{s^2 - 4p}{f^2}\right) \\ &+ \frac{1}{4} \sum_{\substack{[E]_{\mathbb{F}_p} \in \text{Ell}_{\mathbb{F}_p} \\ j(E)=1728}} a(E)^n + \frac{1}{3} \sum_{\substack{[E]_{\mathbb{F}_p} \in \text{Ell}_{\mathbb{F}_p} \\ j(E)=0}} a(E)^n. \end{aligned}$$

*Proof.* First, notice that  $h$  and  $h^*$  agree unless the argument  $\frac{s^2 - 4p}{f^2} = -3$  or  $-4$ , since in all other cases  $w(d) = 1$ . When  $\frac{s^2 - 4p}{f^2} = -4$ , we have the maximal order  $\mathbb{Z}[i]$  and  $h^*(-4) = \frac{h(-4)}{w(-4)} = \frac{1}{2}$ , so  $h(-4) = h^*(-4) + \frac{1}{2}$ . On the other hand, when  $\frac{s^2 - 4p}{f^2} = -3$ , we have the maximal order  $\mathbb{Z}[\omega]$  and  $h^*(-3) = \frac{h(-3)}{w(-3)} = \frac{1}{3}$ , so  $h(-3) = h^*(-3) + \frac{2}{3}$ . Thus,

$$(8) \quad \begin{aligned} \sum_{0 < s < 2\sqrt{p}} s^n \sum_{f|\ell} h\left(\frac{s^2 - 4p}{f^2}\right) &= \sum_{0 < s < 2\sqrt{p}} s^n \sum_{f|\ell} h^*\left(\frac{s^2 - 4p}{f^2}\right) \\ &+ \frac{1}{2} \sum_{0 < s < 2\sqrt{p}} s^n \sum_{\substack{f|\ell \\ \frac{s^2 - 4p}{f^2} = -4}} 1 + \frac{2}{3} \sum_{0 < s < 2\sqrt{p}} s^n \sum_{\substack{f|\ell \\ \frac{s^2 - 4p}{f^2} = -3}} 1. \end{aligned}$$

To complete the proof, we must verify two identities:

$$(9) \quad \sum_{0 < s < 2\sqrt{p}} s^n \sum_{\substack{f|\ell \\ \frac{s^2-4p}{f^2} = -4}} 1 = \frac{1}{2} \sum_{\substack{[E]_{\mathbb{F}_p} \in \text{Ell}_{\mathbb{F}_p} \\ j(E)=1728}} a(E)^n,$$

$$(10) \quad \sum_{0 < s < 2\sqrt{p}} s^n \sum_{\substack{f|\ell \\ \frac{s^2-4p}{f^2} = -3}} 1 = \frac{1}{2} \sum_{\substack{[E]_{\mathbb{F}_p} \in \text{Ell}_{\mathbb{F}_p} \\ j(E)=0}} a(E)^n.$$

First, we consider (9). Using known formulas for  $a(E)$  in the case of curves with  $j$ -invariant 1728 (see Chapter 18 of [10]), one can show that  $a(E) = \pm 2a, \pm 2b$  for all  $E$  appearing in (9). Also, it is easy to verify that  $s = |2a|, |2b|$  satisfy  $\frac{s^2-4p}{\ell^2} = -4$  (with  $\ell = |b|, |a|$ , respectively). Now, suppose  $0 < s < 2\sqrt{p}$  satisfies  $\frac{s^2-4p}{\ell^2} = -4$ . Then  $s^2 - 4p = -4\ell^2$  implies  $s$  is even, so we have  $(\frac{s}{2})^2 + \ell^2 = p$ . Thus, it must be that  $\frac{s}{2} = |a|, |b|$ , since  $\mathbb{Z}[i]$  is a UFD and  $p = a^2 + b^2$ . Since  $n$  is even,  $(2a)^n = (-2a)^n$  and  $(2b)^n = (-2b)^n$ , so (9) follows.

One may complete the proof by showing (10) in a similar manner, first verifying that  $a(E) = \pm(c+d), \pm(2c-d), \pm(c-2d)$  for all  $E$  appearing in the right-hand sum. Details of this proof may be found in [7].  $\square$

**Proposition 5.4.** *Let  $p \equiv 1 \pmod{12}$  be prime and notation as above. Then for  $n \geq 2$  even,*

$$\begin{aligned} \sum_{t=2}^{p-1} a(t, p)^n &= \sum_{0 < s < 2\sqrt{p}} s^n \sum_{f|\ell} h^* \left( \frac{s^2 - 4p}{f^2} \right) \\ &\quad - 2^{n-1}(a^n + b^n) - \frac{1}{3}[(c+d)^n + (2c-d)^n + (c-2d)^n]. \end{aligned}$$

*Proof.* Notice that since  $j(E_t) = \frac{1728}{t}$ , each  $E_t$  represents a distinct isomorphism class of elliptic curves in  $\text{Ell}_{\mathbb{F}_p}$  as  $t$  ranges from 2 to  $p-1$ . Moreover, since  $j(E_t)$  gives an automorphism of  $\mathbb{P}^1$ , every  $j$ -invariant other than 0 and 1728 is represented precisely once. Thus, for even  $n \geq 2$ , we have

$$\sum_{t=2}^{p-1} a(t, p)^n = \sum_{\substack{[E]_{\mathbb{F}_p} \in \text{Ell}_{\mathbb{F}_p}; E/\mathbb{F}_p \\ j(E) \neq 0, 1728}} a(E)^n.$$

For elliptic curves  $E$  with  $j(E) \neq 0, 1728$ , each class  $[E] \in \text{Ell}_{\mathbb{F}_p}$  gives rise to two distinct classes in  $\text{Ell}_{\mathbb{F}_p}$  (see Lemma 4.3), represented by  $E$  and its quadratic twist  $E^{tw}$ . For such curves,  $a(E)$  and  $a(E^{tw})$  differ only by a sign, and so  $a(E)^n = a(E^{tw})^n$ , since  $n$  is even. Therefore, we have

$$\sum_{t=2}^{p-1} a(t, p)^n = \sum_{\substack{[E]_{\mathbb{F}_p} \in \text{Ell}_{\mathbb{F}_p}; E/\mathbb{F}_p \\ j(E) \neq 0, 1728}} a(E)^n = \frac{1}{2} \sum_{\substack{[E]_{\mathbb{F}_p} \in \text{Ell}_{\mathbb{F}_p} \\ j(E) \neq 0, 1728}} a(E)^n.$$

Then, if we add and subtract the contributions from the classes  $[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p}$  with  $j(E) = 0, 1728$ , we have

$$(11) \quad \sum_{t=2}^{p-1} a(t, p)^n = \frac{1}{2} \left[ \sum_{[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p}} a(E)^n - \sum_{\substack{[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p} \\ j(E)=1728}} a(E)^n - \sum_{\substack{[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p} \\ j(E)=0}} a(E)^n \right].$$

Now we look more closely at the first sum on the right. By Hasse's theorem,  $Ell_{\mathbb{F}_p}$  is the disjoint union over  $0 \leq s < 2\sqrt{p}$  of  $I(s, p)$ , where  $I(s, p)$  is defined as in (6). Then since  $n \geq 2$  is even, we may write

$$\sum_{[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p}} a(E)^n = \sum_{0 \leq s < 2\sqrt{p}} \sum_{[E]_{\mathbb{F}_p} \in I(s, p)} s^n = \sum_{0 < s < 2\sqrt{p}} \#I(s, p) s^n,$$

since  $s = 0$  makes no contribution. Substituting this into (11) gives

$$\sum_{t=2}^{p-1} a(t, p)^n = \frac{1}{2} \sum_{0 < s < 2\sqrt{p}} \#I(s, p) s^n - \frac{1}{2} \sum_{\substack{[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p} \\ j(E)=1728}} a(E)^n - \frac{1}{2} \sum_{\substack{[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p} \\ j(E)=0}} a(E)^n.$$

Now we may apply Theorem 4.1 to obtain

$$\sum_{t=2}^{p-1} a(t, p)^n = \sum_{0 < s < 2\sqrt{p}} H(s^2 - 4p) s^n - \frac{1}{2} \sum_{\substack{[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p} \\ j(E)=1728}} a(E)^n - \frac{1}{2} \sum_{\substack{[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p} \\ j(E)=0}} a(E)^n.$$

Using (7) to define  $\ell$ , (5) implies  $H(s^2 - 4p) = \sum_{f|\ell} h\left(\frac{s^2 - 4p}{f^2}\right)$ , which gives

$$\sum_{t=2}^{p-1} a(t, p)^n = \sum_{0 < s < 2\sqrt{p}} s^n \sum_{f|\ell} h\left(\frac{s^2 - 4p}{f^2}\right) - \frac{1}{2} \sum_{\substack{[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p} \\ j(E)=1728}} a(E)^n - \frac{1}{2} \sum_{\substack{[E]_{\mathbb{F}_p} \in Ell_{\mathbb{F}_p} \\ j(E)=0}} a(E)^n.$$

To complete the proof, we apply Lemma 5.3 to the right side to replace  $h$  by  $h^*$ . We finish by collecting terms and applying Lemmas 5.1 and 5.2.  $\square$

Proposition 5.4 and Theorem 4.2 give us the tools necessary to complete the proof of our second main theorem:

*Proof of Theorem 1.3.* By Theorem 4.2, we have for  $k \geq 4$  even,

$$\begin{aligned} \mathrm{Tr}_k(\Gamma, p) &= -1 - \frac{1}{2} h^*(-4p) (-p)^{\frac{k}{2}-1} - (-p)^{\frac{k}{2}-1} \sum_{0 < s < 2\sqrt{p}} 1 \sum_f h^*\left(\frac{s^2 - 4p}{f^2}\right) \\ &\quad - \sum_{j=0}^{\frac{k}{2}-2} (-1)^j \binom{k-2-j}{j} p^j \sum_{0 < s < 2\sqrt{p}} s^{k-2j-2} \sum_f h^*\left(\frac{s^2 - 4p}{f^2}\right), \end{aligned}$$

after substituting in the definition of  $G_k(s, p)$ . Now, note that taking  $k = 2$  in Theorem 4.2 provides

$$\sum_{0 < s < 2\sqrt{p}} 1 \sum_f h^*\left(\frac{s^2 - 4p}{f^2}\right) = p - \frac{1}{2} h^*(-4p).$$

We apply this together with Proposition 5.4 and obtain

$$\begin{aligned} \mathrm{Tr}_k(\Gamma, p) &= -1 + (-p)^{\frac{k}{2}-1} \cdot (-p) - \sum_{j=0}^{\frac{k}{2}-2} (-1)^j \binom{k-2-j}{j} p^j \sum_{t=2}^{p-1} a(t, p)^{k-2j-2} \\ &\quad - \frac{1}{2} \sum_{j=0}^{\frac{k}{2}-2} (-1)^j \binom{k-2-j}{j} p^j [(2a)^{k-2j-2} + (2b)^{k-2j-2}] \\ &\quad - \frac{1}{3} \sum_{j=0}^{\frac{k}{2}-2} (-1)^j \binom{k-2-j}{j} p^j [(c+d)^{k-2j-2} + (2c-d)^{k-2j-2} \\ &\quad \quad \quad + (c-2d)^{k-2j-2}]. \end{aligned}$$

Now, we notice the simple fact that

$$(-p)^{\frac{k}{2}-1} \cdot (-p) = -(-p)^{\frac{k}{2}-1}(p-2) - 2 \left( \frac{1}{2}(-p)^{\frac{k}{2}-1} \right) - 3 \left( \frac{1}{3}(-p)^{\frac{k}{2}-1} \right).$$

Splitting up the factors of  $(-p)^{\frac{k}{2}-1}$  in this way gives that

$$\begin{aligned} \mathrm{Tr}_k(\Gamma, p) &= -1 - \lambda(k, p) - \sum_{t=2}^{p-1} (-p)^{\frac{k}{2}-1} - \sum_{t=2}^{p-1} \sum_{j=0}^{\frac{k}{2}-2} (-1)^j \binom{k-2-j}{j} p^j a(t, p)^{k-2j-2} \\ &= -1 - \lambda(k, p) - \sum_{t=2}^{p-1} G_k(a(t, p), p). \quad \square \end{aligned}$$

*Remark 5.5.* Note that using Theorem 1.2, we may reformulate Theorem 1.3 in terms of the hypergeometric function  ${}_2F_1\left(\begin{smallmatrix} \xi, \xi^5 \\ \varepsilon \end{smallmatrix} \middle| t\right)$ .

## 6. PROOF OF THEOREM 1.4

Theorem 1.4 is proved by combining Theorems 1.2 and 1.3 with an inverse pair given in [15]. First, recalling (4), let  $m = \frac{k}{2} - 1$  and  $H_m(x) := \sum_{i=0}^m \binom{m+i}{m-i} x^i$ . Then

$$(12) \quad G_k(s, p) = (-p)^m H_m\left(\frac{-s^2}{p}\right).$$

Now, we make use of the inverse pair [15, p. 67] given by

$$(13) \quad \rho_n(x) = \sum_{k=0}^n \binom{n+k}{n-k} x^k, \quad x^n = \sum_{k=0}^n (-1)^{k+n} \left[ \binom{2n}{n-k} - \binom{2n}{n-k-1} \right] \rho_k(x).$$

Applied to the definition of  $H_m$ , this gives

$$x^m = \sum_{i=0}^m (-1)^{i+m} \left[ \binom{2m}{m-i} - \binom{2m}{m-i-1} \right] H_i(x).$$

By taking  $x = \frac{-s^2}{p}$ , together with (12), we have

$$(14) \quad s^{2m} = \sum_{i=0}^m p^{m-i} \left[ \binom{2m}{m-i} - \binom{2m}{m-i-1} \right] G_{2i+2}(s, p) = \sum_{i=0}^m b_i G_{2i+2}(s, p),$$

where  $b_i$  is as defined in the statement of Theorem 1.4.

*Proof of Theorem 1.4.* By (14), we have

$$(15) \quad s^{2m} = \sum_{i=0}^m b_i G_{2i+2}(s, p) = G_{2m+2}(s, p) + \sum_{i=0}^{m-1} b_i G_{2i+2}(s, p),$$

since  $b_m = 1$ . Now, for  $m \geq 1$ , Theorem 1.3 coupled with (15) implies

$$\begin{aligned} \mathrm{Tr}_{2(m+1)}(\Gamma, p) &= -1 - \lambda(2m+2, p) - \sum_{t=2}^{p-1} \left( a(t, p)^{2m} - \sum_{i=0}^{m-1} b_i G_{2i+2}(a(t, p), p) \right) \\ &= -1 - \lambda(2m+2, p) - \sum_{t=2}^{p-1} a(t, p)^{2m} + b_0 \sum_{t=2}^{p-1} G_2(a(t, p), p) \\ &\quad + \sum_{i=1}^{m-1} b_i \sum_{t=2}^{p-1} G_{2i+2}(a(t, p), p) \\ &= -1 - \lambda(2m+2, p) - \sum_{t=2}^{p-1} a(t, p)^{2m} + b_0(p-2) \\ &\quad - \sum_{i=1}^{m-1} b_i (\mathrm{Tr}_{2i+2}(\Gamma, p) + 1 + \lambda(2i+2, p)), \end{aligned}$$

since  $G_2 = 1$ . The proof is completed by rearranging and noting that Theorem 1.2 implies  $a(t, p)^{2m} = p^{2m} \phi^m (1-t)_2 F_1 \left( \xi, \xi^5 \middle| t \right)^{2m}$ .  $\square$

## 7. $\tau(p)$ COROLLARIES

Specializing to various values of  $k$  in Theorem 1.3, we arrive at more explicit formulas. In particular, by taking  $k = 12$  we obtain a formula for Ramanujan's  $\tau$ -function. Recall that we define  $\tau(n)$  by

$$(2\pi)^{-12} \Delta(z) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n.$$

Also, recall that  $\Delta(z)$  generates the one-dimensional space  $S_{12}$ , and thus  $\mathrm{Tr}_{12}(\Gamma, p) = \tau(p)$  for primes  $p$ . We conclude with results that stem from the case  $k = 12$ .

Throughout, we let  $a, b \in \mathbb{Z}$  be such that  $p = a^2 + b^2$  and  $a + bi \equiv 1 (2 + 2i)$  in  $\mathbb{Z}[i]$ . Further, let  $c, d \in \mathbb{Z}$  satisfy  $p = c^2 - cd + d^2$  and  $c + d\omega \equiv 2 (3)$  in  $\mathbb{Z}[\omega]$ , where  $\omega = e^{2\pi i/3}$ . The first corollary follows easily from Theorem 1.3.

**Corollary 7.1.** *Let  $a, b, c$ , and  $d$  be as defined above, and set  $x = a^2 b^2$  and  $y = cd$ . If  $p$  is a prime,  $p \equiv 1 (12)$ , then*

$$\tau(p) = -1 - 8p^5 + 80p^3 x - 256p x^2 + 27y^2 p^3 - 27y^3 p^2 - \sum_{t=2}^{p-1} G_{12}(a(t, p), p),$$

where  $G_{12}(s, p) = s^{10} - 9ps^8 + 28p^2 s^6 - 35p^3 s^4 + 15p^4 s^2 - p^5$ .

By combining Corollary 7.1 with Theorems 1.2 and 1.3, we can inductively arrive at a formula for  $\tau(p)$  in terms of only 10th powers of  ${}_2F_1 \left( \xi, \xi^5 \middle| t \right)$ :

**Corollary 7.2.** *Let  $p \equiv 1 \pmod{12}$  be prime and let  $a, b, c,$  and  $d$  be defined as above. Let  $\xi$  be an element of order 12 in  $\widehat{\mathbb{F}_p^\times}$ . Then*

$$\begin{aligned} \tau(p) &= 42p^6 - 90p^4 - 75p^3 - 35p^2 - 9p - 1 - 2^9(a^{10} + b^{10}) \\ &\quad - \frac{1}{3}((c+d)^{10} + (2c-d)^{10} + (c-2d)^{10}) - \sum_{t=2}^{p-1} p^{10} \phi(1-t) {}_2F_1\left(\xi, \xi^5 \middle| t\right)^{10}. \end{aligned}$$

*Proof.* We sketch the proof here, but refer the reader to [7] for complete details. One must begin with explicit computations for  $G_k(s, p)$  and  $\lambda(k, p)$ , for even  $k = 2, \dots, 12$ . The formula is built by using these, together with Theorem 1.3 and the fact that  $\text{Tr}_k(\Gamma, p) = 0$  for even  $k = 2, \dots, 10$ . For example, since  $G_4(s, p) = s^2 - p$  and  $\lambda(4, p) = 2p$ , Theorem 1.3 implies

$$0 = \text{Tr}_4(\Gamma, p) = -1 - 2p + p(p-2) - \sum_{t=2}^{p-1} a(t, p)^2,$$

and so

$$(16) \quad 0 = p^2 - 4p - 1 - \sum_{t=2}^{p-1} a(t, p)^2.$$

We use this to derive a formula for  $\sum_{t=2}^{p-1} a(t, p)^4$ . For  $k = 6$ , we have  $G_6(s, p) = s^4 - 3ps^2 + p^2$  and again  $\text{Tr}_6(\Gamma, p) = 0$ . After computing  $\lambda(6, p)$ , Theorem 1.3 gives

$$0 = \text{Tr}_6(\Gamma, p) = -1 + 4p^2 - 2^3(a^4 + b^4) - \sum_{t=2}^{p-1} (a(t, p)^4 - 3pa(t, p)^2 + p^2).$$

Using (16) and simplifying, we get

$$(17) \quad 0 = 2p^3 - 6p^2 - 3p - 2^3(a^4 + b^4) - 1 - \sum_{t=2}^{p-1} a(t, p)^4.$$

We continue this process, using successive formulas for  $G_k(s, p)$  and  $\lambda(k, p)$  to derive formulas for sums of  $a(t, p)^k$  for even  $k = 2, \dots, 8$ . Using the technique a final time, we combine these with the fact that  $\text{Tr}_{12}(\Gamma, p) = \tau(p)$  to arrive at a formula for  $\tau(p)$  in terms of 10th powers of  $a(t, p)$ . The end result is then achieved by using Theorem 1.2 to convert from  $a(t, p)$  to the desired hypergeometric function.  $\square$

We close with one final formula for  $\tau(p)$ .

**Corollary 7.3.** *Let  $p \equiv 1 \pmod{12}$  be prime and let  $a, b, c,$  and  $d$  be defined as above. Let  $\xi$  be an element of order 12 in  $\widehat{\mathbb{F}_p^\times}$ . Then*

$$\begin{aligned} \tau(p) &= 12p^6 - 27p^4 - 25p^3 - 14p^2 - \frac{54}{11}p - 1 - \frac{1}{11p} - \frac{2^{11}}{11p}(a^{12} + b^{12}) \\ &\quad - \frac{1}{33p}((c+d)^{12} + (2c-d)^{12} + (c-2d)^{12}) - \frac{1}{11} \sum_{t=2}^{p-1} p^{11} {}_2F_1\left(\xi, \xi^5 \middle| t\right)^{12}. \end{aligned}$$

*Proof.* The proof follows as in Corollary 7.2, but by taking  $k = 14$ . First, we have

$$G_{14}(s, p) = s^{12} - 11ps^{10} + 45p^2s^8 - 84p^3s^6 + 70p^4s^4 - 21p^5s^2 + p^6.$$

Then, since  $\text{Tr}_{14}(\Gamma, p) = 0$ , Theorem 1.3 implies

$$0 = -1 - \lambda(14, p) - \sum_{t=2}^{p-1} G_{14}(a(t, p), p).$$

Now, one applies the formulas for  $\sum_{t=2}^{p-1} a(t, p)^k$  derived for even  $k = 2, \dots, 10$ , together with a formula for  $\lambda(14, p)$ , to complete the proof.  $\square$

## REFERENCES

- [1] S. Ahlgren, *The points of a certain fivefold over finite fields and the twelfth power of the eta function*, Finite Fields Appl. **8** (2002), no. 1, 18-33. MR1872789 (2002h:11056)
- [2] S. Ahlgren and K. Ono, *Modularity of a certain Calabi-Yau threefold*, Monatsh. Math. **129** (2000), no. 3, 177-190. MR1746757 (2001b:11059)
- [3] S. Ahlgren and K. Ono, *A Gaussian hypergeometric series evaluation and Apéry number congruences*, J. Reine Angew. Math. **518** (2000), 187-212. MR1739404 (2001c:11057)
- [4] F. Beukers, *Algebraic values of G-functions*, J. Reine Angew. Math. **434** (1993), 45-65. MR1195690 (94d:11055)
- [5] D.A. Cox, *Primes of the form  $x^2 + ny^2$* . In *Fermat, Class Field Theory and Complex Multiplication*, John Wiley & Sons, New York, 1989. MR1028322 (90m:11016)
- [6] S. Frechette, K. Ono, and M. Papanikolas, *Gaussian hypergeometric functions and traces of Hecke operators*, Int. Math. Res. Not. (2004), no. 60, 3233-3262. MR2096220 (2006a:11055)
- [7] J.G. Fuselier, *Hypergeometric functions over finite fields and relations to modular forms and elliptic curves*, Ph.D. thesis, Texas A&M University, 2007.
- [8] J. Greene, *Hypergeometric functions over finite fields*, Trans. Amer. Math. Soc. **301** (1987), no. 1, 77-101. MR879564 (88e:11122)
- [9] 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), no. 418. MR960090 (90d:11056)
- [10] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990. MR1070716 (92e:11001)
- [11] M. Koike, *Hypergeometric series over finite fields and Apéry numbers*, Hiroshima Math. J. **22** (1992), no. 3, 461-467. MR1194045 (93i:11146)
- [12] S. Lang, *Cyclotomic Fields I and II*, Graduate Texts in Mathematics, vol. 121, Springer-Verlag, New York, 1990. MR1029028 (91c:11001)
- [13] K. Ono, *Values of Gaussian hypergeometric series*, Trans. Amer. Math. Soc. **350** (1998), no. 3, 1205-1223. MR1407498 (98e:11141)
- [14] M. Papanikolas, *A formula and a congruence for Ramanujan's  $\tau$ -function*, Proc. Amer. Math. Soc. **134** (2006), no. 2, 333-341. MR2175999 (2007d:11046)
- [15] J. Riordan, *Combinatorial Identities*, John Wiley & Sons, New York, 1968. MR0231725 (38:53)
- [16] R. Schoof, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory, Ser. A **46** (1987), no. 2, 183-211. MR914657 (88k:14013)
- [17] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986. MR817210 (87g:11070)
- [18] P.F. Stillier, *Classical automorphic forms and hypergeometric functions*, J. Number Theory **28** (1988), no. 2, 219-232. MR927661 (89b:11037)

UNITED STATES MILITARY ACADEMY, 646 SWIFT ROAD, WEST POINT, NEW YORK 10996

*E-mail address:* jenny.fuselier@usma.edu

*Current address:* Department of Mathematics & Computer Science, Drawer 31, High Point University, High Point, North Carolina 27262

*E-mail address:* jfuselie@highpoint.edu