

CONGRUENCES FOR ${}_3F_2$ HYPERGEOMETRIC FUNCTIONS OVER FINITE FIELDS

KEN ONO AND DAVID PENNISTON

In the 1980's, J. Greene [G1, G2] initiated a study of finite field hypergeometric functions, and he found that they satisfy a variety of properties analogous to those of their classical counterparts. Recent works by S. Ahlgren and K. Ono [A-O, O] and M. Koike [K] have illustrated that certain special values of these functions are congruent to Apéry type numbers modulo the characteristic of the finite field. Here we present congruences of a different type which relate the values of these functions to a simple polynomial in the characteristic.

We begin by recalling Greene's definition. As usual, let $GF(p)$ denote the finite field with p elements. We extend all characters χ of $GF(p)^\times$ to $GF(p)$ by setting $\chi(0) := 0$. If A and B are two characters of $GF(p)$, then we denote the normalized Jacobi sum by

$$(1) \quad \binom{A}{B} := \frac{B(-1)}{p} J(A, \bar{B}) = \frac{B(-1)}{p} \sum_{x \in GF(p)} A(x) \bar{B}(1-x).$$

Definition 1. *If A_0, A_1, \dots, A_n , and B_1, B_2, \dots, B_n are characters of $GF(p)$, then Greene's hypergeometric function ${}_{n+1}F_n \left(\begin{matrix} A_0, & A_1, & \dots, & A_n \\ B_1, & \dots, & B_n \end{matrix} \middle| x \right)_p$ is defined by*

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

where the summation is over all characters χ of $GF(p)$.

We restrict our attention to the ${}_{n+1}F_n \left(\begin{matrix} \phi_p, & \phi_p, & \dots, & \phi_p \\ \epsilon_p, & \dots, & \epsilon_p \end{matrix} \middle| \lambda \right)_p$ functions, where ϕ_p denotes the Legendre symbol modulo p and ϵ_p is the trivial character; for convenience we denote these functions by ${}_{n+1}F_n(\lambda)_p$. S. Ahlgren and the first author [A-O] proved one of F. Beukers' Apéry number super-congruences by explicitly evaluating all of the ${}_4F_3(1)_p$

1991 *Mathematics Subject Classification.* Primary 11T24.

Key words and phrases. Gaussian hypergeometric functions.

The first author thanks the National Science Foundation, the Alfred P. Sloan Foundation, and the David and Lucile Packard Foundation.

and relating these values to the zeta function of a specific Calabi-Yau manifold. It is also shown that if p is an odd prime, then [Theorem 3, A-O]

$${}_4F_3(1)_p \equiv -1 - p^{13} - p^{14} \pmod{32}.$$

Here we obtain many such congruences for ${}_3F_2(\lambda)_p$. For example, if $p \neq 2, 3, 5, 11$, then

$$(2) \quad {}_3F_2\left(\frac{2673}{2048}\right)_p \equiv \phi_p(-2)(1 + p^{-1} + p^{-2}) \equiv \phi_p(-2)(1 + p^6 + p^7) \pmod{20}.$$

We begin by defining groups G_i , functions $\lambda_i(s)$ and sets S_i as follows.

i	G_i	$\lambda_i(s)$	S_i
1	$\mathbb{Z}2$	s	$0, 4, \frac{9}{2}$
2	$\mathbb{Z}2 \times \mathbb{Z}2$	$\frac{4}{1-s^2}$	$0, \pm 1, \pm \frac{1}{3}$
3	$\mathbb{Z}4$	$\frac{(8s+1)^2}{16s^2}$	$0, -\frac{1}{8}, -\frac{1}{16}$
4	$\mathbb{Z}2 \times \mathbb{Z}4$	$\frac{4(16s^2+1)^2}{(4s+1)^2(4s-1)^2}$	$0, \pm \frac{1}{4}$
5	$\mathbb{Z}2 \times \mathbb{Z}4$	$-\frac{(16s^2-24s+1)^2}{16s(4s-1)^2}$	$0, \frac{1}{4}$
6	$\mathbb{Z}2 \times \mathbb{Z}8$	$\frac{(4096s^8+8192s^7+6144s^6+2048s^5+512s^4+256s^3+96s^2+16s+1)^2}{256(4s+1)^4(2s+1)^4s^4}$	$0, -\frac{1}{4}, -\frac{1}{2}$
7	$\mathbb{Z}2 \times \mathbb{Z}8$	$-\frac{4(2048s^8+4096s^7+3072s^6+1024s^5-128s^4-256s^3-96s^2-16s-1)^2}{(8s^2+8s+1)(8s^2-1)(8s^2+4s+1)^2(4s+1)^4}$	$0, -\frac{1}{4}, -\frac{1}{2}$
8	$\mathbb{Z}2 \times \mathbb{Z}8$	$\frac{(8192s^8+16384s^7+12288s^6+4096s^5+256s^4-256s^3-96s^2-16s-1)^2}{256s^4(8s^2+8s+1)(8s^2-1)(8s^2+4s+1)^2(2s+1)^4}$	$0, -\frac{1}{4}, -\frac{1}{2}$
9	$\mathbb{Z}8$	$\frac{(8s^4-16s^3+16s^2-8s+1)^2}{16(s-1)^4s^4}$	$0, \frac{1}{2}, 1$
10	$\mathbb{Z}6$	$-\frac{(3s^2-6s-1)^2}{16s^3}$	$0, -1, -\frac{1}{9}$
11	$\mathbb{Z}2 \times \mathbb{Z}6$	$\frac{(s^4-12s^3+30s^2+228s-759)^2}{128(s-5)^3(s-3)(s+3)}$	$1, \pm 3, 5, 9$
12	$\mathbb{Z}2 \times \mathbb{Z}6$	$-\frac{(s^4-12s^3+30s^2-156s+393)^2}{128(s-1)^3(s-9)(s-3)}$	$1, \pm 3, 5, 9$
13	$\mathbb{Z}2 \times \mathbb{Z}6$	$\frac{4(s^4-12s^3+30s^2+36s-183)^2}{(s-5)^3(s-1)^3(s-9)(s+3)}$	$1, \pm 3, 5, 9$
14	$\mathbb{Z}10$	$\frac{(2s^2-2s+1)^2(4s^4-12s^3+6s^2+2s-1)^2}{16(s-1)^5(s^2-3s+1)s^5}$	$0, \frac{1}{2}, 1$
15	$\mathbb{Z}12$	$\frac{(24s^8-96s^7+216s^6-312s^5+288s^4-168s^3+60s^2-12s+1)^2}{16(s-1)^6(3s^2-3s+1)^2s^6}$	$0, \frac{1}{2}, 1$

If p is prime and n is a nonzero integer, then $\text{ord}_p(n)$ shall denote the power of p dividing n ; extend ord_p to \mathbb{Q} in the obvious way.

Theorem 1. For each i in the preceding table, define N_i by

$$N_i := \begin{cases} 2|G_i| & \text{if } 4 \nmid |G_i|, \\ 4|G_i| & \text{otherwise.} \end{cases}$$

If $s \in \mathbb{Q} - S_i$ and $p \geq 5$ is a prime for which

$$\text{ord}_p(\lambda_i(s)(\lambda_i(s) - 4)) = \text{ord}_p(N_i) = 0,$$

then

$${}_3F_2\left(\frac{4}{4 - \lambda_i(s)}\right)_p \equiv \phi_p(\lambda_i^2(s) - 4\lambda_i(s))(1 + p^{-1} + p^{-2}) \pmod{N_i}.$$

Remark. Example (2) is obtained by letting $s = 3/4$ when $i = 14$ in Theorem 1.

2. PROOF OF THEOREM 1

If $\lambda \in \mathbb{Q} - \{0, 4\}$, define the elliptic curve $E(\lambda)/\mathbb{Q}$ by the equation

$$(3) \quad E(\lambda) : y^2 = (x - 1) \left(x^2 + \frac{4 - \lambda}{\lambda} \right).$$

The point $(1, 0)$ is a point of order 2 on $E(\lambda)$. (Note. This curve is isomorphic over \mathbb{Q} to the curve given in [(16), O]). This elliptic curve has discriminant

$$(4) \quad \Delta(E(\lambda)) := 1024\lambda^{-3}(\lambda - 4)$$

and j -invariant

$$(5) \quad j(E(\lambda)) := \frac{256(\lambda - 3)^3}{\lambda - 4}.$$

If p is a prime such that $\text{ord}_p(\Delta(E(\lambda))) = 0$, then $E(\lambda)$ is an elliptic curve when considered over $GF(p)$; in this case we say that $E(\lambda)$ has *good reduction at p* , and define ${}_3a_2(p; \lambda)$ by

$$(6) \quad {}_3a_2(p; \lambda) = p + 1 - |E(\lambda)_p|,$$

where $|E(\lambda)_p|$ denotes the order of the Mordell-Weil group of $E(\lambda)$ over $GF(p)$.

Extending a result of J. Greene and D. Stanton [G-S], the first author proved the following theorem in [O].

Theorem 2. *If $\lambda \in \mathbb{Q} - \{0, 4\}$ and $p \geq 5$ is a prime for which $\text{ord}_p(\lambda(\lambda - 4)) = 0$, then*

$${}_3F_2\left(\frac{4}{4-\lambda}\right)_p = \frac{\phi_p(\lambda^2 - 4\lambda)({}_3a_2(p; \lambda)^2 - p)}{p^2}.$$

Theorem 1 follows from Theorem 2 and the following elementary proposition regarding the numbers ${}_3a_2(p; \lambda) \pmod{N}$ when $E(\lambda)$ is the twist of an elliptic curve over \mathbb{Q} whose Mordell-Weil group has a torsion subgroup of order N .

Proposition 3. *Suppose that E/\mathbb{Q} is an elliptic curve for which $j(E) = j(E(\lambda)) \neq 1728$, and assume the torsion subgroup of E/\mathbb{Q} has even order N . Let $N' = 2N$ if $4 \nmid N$, and $N' = 4N$ if $4 \mid N$. If $p \geq 5$ is a prime for which E has good reduction and*

$$\text{ord}_p(\lambda(\lambda - 4)) = \text{ord}_p(N) = 0,$$

then

$${}_3F_2\left(\frac{4}{4-\lambda}\right)_p \equiv \phi_p(\lambda^2 - 4\lambda)(1 + p^{-1} + p^{-2}) \pmod{N'}.$$

Proof. By (4), the condition that the odd prime p satisfies $\text{ord}_p(\lambda(\lambda - 4)) = 0$ implies that $E(\lambda)$ is an elliptic curve over $GF(p)$. And since $j(E) = j(E(\lambda))$, E is a twist of $E(\lambda)$ (see [III, Proposition 1.4 (b), Si]).

We claim that in fact E is a quadratic twist of $E(\lambda)$. To see this, note first that if $j(E) \neq 0, 1728$, then our claim is given by [X, Proposition 5.4(i), Si]. In case $j(E) = 0$, we know that E is given by an equation of the form $E : y^2 = x^3 - b$, $b \in \mathbb{Q} - \{0\}$. And since N is even, $b = c^3$ for some $c \in \mathbb{Q} - \{0\}$ (so the point $(c, 0)$ has order 2). The same argument holds for $E(\lambda)$; indeed, one can check (since $\lambda = 3$ in this case) that $E(\lambda)$ is given by the equation $y^2 = x^3 - \frac{8}{27}$. Therefore E is the $\frac{3c}{2}$ -quadratic twist of $E(\lambda)$.

If E_p denotes the curve E considered over $GF(p)$, this implies that

$$(7) \quad {}_3a_2(p; \lambda) = \pm(p + 1 - |E_p|).$$

Now, the fact that $\text{ord}_p(N) = 0$ gives that the reduction map $E \rightarrow E_p$ is injective on the torsion points of E/\mathbb{Q} (see [VII, Proposition 3.1 (b), Si]), and hence

$$|E_p| \equiv 0 \pmod{N}.$$

Therefore, by (7) we find that

$${}_3a_2(p; \lambda) \equiv \pm(p + 1) \pmod{N}.$$

The claim now follows easily from Theorem 2. \square

Proof of Theorem 1. We prove Theorem 1 in the case when $i = 10$ (i.e. $G_{10} = \mathbb{Z}6$); the remaining cases follow *mutatis mutandis*. Notice that the groups G_i are exactly those which

occur as torsion subgroups of elliptic curves over \mathbb{Q} and have an element of order 2 (see, for example, [VIII, Theorem 7.5, Si]).

Kubert [Ku] has shown that any elliptic curve E/\mathbb{Q} having a rational point of order 6 can be given by an equation of the form

$$(8) \quad E : y^2 + (1 - s)xy - (s^2 + s)y = x^3 - (s^2 + s)x^2,$$

where $s \in \mathbb{Q} - \{0, -1, -1/9\}$. This curve has discriminant

$$(9) \quad \Delta(E) = s^6(s + 1)^3(9s + 1),$$

and its j -invariant is

$$j(E) = \frac{(9s^4 + 12s^3 + 30s^2 + 12s + 1)^3}{s^6(s + 1)^3(9s + 1)}.$$

Setting this equal to $j(E(\lambda))$, we obtain one rational solution $\lambda = \lambda_{10}(s)$, which is given in the table. By Proposition 3, for every $s \in \mathbb{Q} - S_{10}$ and every prime $p \geq 5$ for which $\text{ord}_p(\lambda_{10}(s)(\lambda_{10}(s) - 4)) = 0$ and E has good reduction at p , we have

$${}_3F_2 \left(\frac{4}{4 - \lambda_{10}(s)} \right) \equiv \phi_p(\lambda_{10}(s)^2 - 4\lambda_{10}(s))(1 + p^{-1} + p^{-2}) \pmod{12}.$$

Since

$$\lambda_{10}(s)(\lambda_{10}(s) - 4) = \frac{(3s^2 - 6s - 1)^2(9s + 1)(s + 1)^3}{256s^6},$$

by (9) we find that all the potential odd primes of bad reduction for E already have the property that $\text{ord}_p(\lambda_{10}(s)(\lambda_{10}(s) - 4)) \neq 0$. This completes the proof when $i = 10$.

Theorem 1 is obtained by arguing as above for all the possible torsion subgroups of elliptic curves E/\mathbb{Q} containing a rational point of order 2. All such curves have a convenient parameterization as in (8), and they are listed in [Table 3, Ku]. \square

REFERENCES

[A-O] S. Ahlgren and K. Ono, *A Gaussian hypergeometric series evaluation and Apéry number congruences*, J. reine angew. math. **518** (2000), 187-212.
 [G1] J. Greene, *Character sum analogues for hypergeometric and generalized hypergeometric functions over finite fields*, Ph.D. thesis, University of Minnesota, 1984.
 [G2] J. Greene, *Hypergeometric series over finite fields*, Trans. Amer. Math. Soc. **301**, **1** (1987), 77-101.
 [G-S] J. Greene and D. Stanton, *A character sum evaluation and Gaussian hypergeometric series*, J. Number Theory **23** (1986), 136-148.
 [K] M. Koike, *Hypergeometric series over finite fields and Apéry numbers*, Hiroshima Math. J. **22** (1992), 461-467.
 [Ku] D. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Society **33** (1976), 193-237.
 [O] K. Ono, *Values of Gaussian hypergeometric series*, Trans. Amer. Math. Soc. **350** (1998), 1205-1223.

[Si] J. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, 1986.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WISCONSIN, MADISON, WISCONSIN 53706
E-mail address: `ono@math.wisc.edu`

DEPARTMENT OF MATHEMATICS, FURMAN UNIVERSITY, GREENVILLE, SOUTH CAROLINA 29613
E-mail address: `david.penniston@furman.edu`