CONGRUENCES FOR ${}_2F_1$ HYPERGEOMETRIC FUNCTIONS OVER FINITE FIELDS

Matthew Boylan

In a recent paper [O-P], K. Ono and D. Penniston established several families of congruences for ${}_3F_2$ hypergeometric functions over finite fields. In this note, we obtain congruences for ${}_2F_1$ hypergeometric functions over finite fields using similar methods. For example, if $p \neq 2, 3, 5, 7$ is prime, then

$$ {}_2F_1\left(\begin{matrix}\phi_p, & \phi_p \\ & \epsilon_p\end{matrix} \,\Big|\, -\frac{81}{175}\right)_p \equiv -\phi_p(7)(1+p^{-1}) \pmod{16}, \tag{1}$$

where ϕ_p is the Legendre symbol modulo p and ϵ_p is the trivial character.

J. Greene [G1, G2] defined finite field hypergeometric functions and developed many of their properties. In what follows, we denote by $GF(p)$ the finite field with p elements, and we extend all characters χ of $GF(p)^*$ to $GF(p)$ by setting $\chi(0) := 0$. Following Greene, the first definition we give is the finite field analogue of the binomial coefficient, and the second definition is the finite field analogue of the classical hypergeometric functions.

Definition 1. *If A and B are characters of $GF(p)$, then*

$$ \binom{A}{B} := \frac{B(-1)}{p} J(A, \overline{B}) = \frac{B(-1)}{p} \sum_{x \in GF(p)} A(x)\overline{B}(1-x), \tag{2}$$

where $J(\chi, \psi)$ denotes the Jacobi sum if χ and ψ are characters of $GF(p)$.

Definition 2. *If $A_0, A_1, ..., A_n$, and $B_1, ..., B_n$ are characters of $GF(p)$, then the hypergeometric function ${}_{n+1}F_n\left(\begin{matrix}A_0, & A_1, & \dots, & A_n \\ & B_1, & \dots, & B_n\end{matrix} \,\Big|\, x\right)_p$ is defined by*

$$ {}_{n+1}F_n\left(\begin{matrix}A_0, & A_1, & \dots, & A_n \\ & B_1, & \dots, & B_n\end{matrix} \,\Big|\, x\right)_p := \frac{p}{p-1} \sum_{\chi} \binom{A_0\chi}{\chi} \binom{A_1\chi}{B_1\chi} \cdots \binom{A_n\chi}{B_n\chi} \chi(x), \tag{3}$$

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

Here we are interested in the functions ${}_2F_1\left(\begin{matrix}\phi_p, & \phi_p \\ & \epsilon_p\end{matrix} \,\Big|\, \lambda\right)_p$ which we denote by ${}_2F_1(\lambda)_p$. We also define the objects G_i, $\lambda_i(s)$, $D_i(s)$, and S_i as the entries given in the table below. These objects parametrize our congruences for the functions ${}_2F_1(\lambda)_p$.

1991 *Mathematics Subject Classification.* Primary 11T24.
Key words and phrases. Gaussian hypergeometric functions.

i	G_i	$\lambda_i(s)$	$D_i(s)$	S_i
1	$\mathbb{Z}2 \times \mathbb{Z}2$	$\frac{r}{s}$	s	$\{0, r\}$
2	$\mathbb{Z}2 \times \mathbb{Z}2$	$-\frac{r-s}{s}$	$-s$	$\{0, r\}$
3	$\mathbb{Z}2 \times \mathbb{Z}2$	$\frac{s}{r}$	r	$\{0, r\}$
4	$\mathbb{Z}2 \times \mathbb{Z}2$	$\frac{r-s}{r}$	$-r$	$\{0, r\}$
5	$\mathbb{Z}2 \times \mathbb{Z}2$	$-\frac{s}{r-s}$	$r-s$	$\{0, r\}$
6	$\mathbb{Z}2 \times \mathbb{Z}2$	$\frac{r}{r-s}$	$-(r-s)$	$\{0, r\}$
7	$\mathbb{Z}2 \times \mathbb{Z}4$	$\frac{16s}{(4s+1)^2}$	1	$\{0, \pm\frac{1}{4}\}$
8	$\mathbb{Z}2 \times \mathbb{Z}4$	$\frac{(4s+1)^2}{(4s-1)^2}$	-1	$\{0, \pm\frac{1}{4}\}$
9	$\mathbb{Z}2 \times \mathbb{Z}4$	$\frac{(4s+1)^2}{16s}$	s	$\{0, \pm\frac{1}{4}\}$
10	$\mathbb{Z}2 \times \mathbb{Z}6$	$-\frac{(s-1)^3(s-9)}{128(s-3)}$	$2(s-3)$	$\{1, \pm3, 5, 9\}$
11	$\mathbb{Z}2 \times \mathbb{Z}6$	$\frac{(s-5)^3(s+3)}{128(s-3)}$	$-2(s-3)$	$\{1, \pm3, 5, 9\}$
12	$\mathbb{Z}2 \times \mathbb{Z}6$	$\frac{(s-1)^3(s-9)}{(s-5)^3(s+3)}$	$(s-5)(s+3)$	$\{1, \pm3, 5, 9\}$
13	$\mathbb{Z}2 \times \mathbb{Z}6$	$\frac{128(s-3)}{(s-5)^3(s+3)}$	$-(s-5)(s+3)$	$\{1, \pm3, 5, 9\}$
14	$\mathbb{Z}2 \times \mathbb{Z}6$	$\frac{(s-5)^3(s+3)}{(s-1)^3(s-9)}$	$(s-1)(s-9)$	$\{1, \pm3, 5, 9\}$
15	$\mathbb{Z}2 \times \mathbb{Z}6$	$-\frac{128(s-3)}{(s-1)^3(s-9)}$	$-(s-1)(s-9)$	$\{1, \pm3, 5, 9\}$
16	$\mathbb{Z}2 \times \mathbb{Z}8$	$-\frac{(8s^2+4s+1)^2(8s^2-1)(8s^2+8s+1)}{(4s+1)^4}$	1	$\{0, -\frac{1}{2}, -\frac{1}{4}\}$
17	$\mathbb{Z}2 \times \mathbb{Z}8$	$\frac{256(2s+1)^4s^4}{(4s+1)^4}$	-1	$\{0, -\frac{1}{2}, -\frac{1}{4}\}$
18	$\mathbb{Z}2 \times \mathbb{Z}8$	$\frac{(8s^2+4s+1)^2(8s^2-1)(8s^2+8s+1)}{256(2s+1)^4s^4}$	1	$\{0, -\frac{1}{2}, -\frac{1}{4}\}$
19	$\mathbb{Z}2 \times \mathbb{Z}8$	$\frac{(4s+1)^4}{256(2s+1)^4s^4}$	-1	$\{0, -\frac{1}{2}, -\frac{1}{4}\}$
20	$\mathbb{Z}2 \times \mathbb{Z}8$	$\frac{256(2s+1)^4s^4}{(8s^2+4s+1)^2(8s^2-1)(8s^2+8s+1)}$	$(8s^2+8s+1)(8s^2-1)$	$\{0, -\frac{1}{2}, -\frac{1}{4}\}$
21	$\mathbb{Z}2 \times \mathbb{Z}8$	$-\frac{(4s+1)^4}{(8s^2+4s+1)^2(8s^2-1)(8s^2+8s+1)}$	$-(8s^2+8s+1)(8s^2-1)$	$\{0, -\frac{1}{2}, -\frac{1}{4}\}$

Furthermore, we define $\mathrm{ord}_p(n)$ to be the power of p dividing n if p is prime and n is any nonzero integer. If $\alpha = \frac{a}{b} \in \mathbb{Q}$, then $\mathrm{ord}_p(\alpha) := \mathrm{ord}_p(a) - \mathrm{ord}_p(b)$.

Theorem 1. *For each i in the preceding table, suppose $r \in \mathbb{Q} \setminus \{0\}$, $s \in \mathbb{Q} \setminus S_i$, and $p \geq 5$ is a prime for which*

$$\mathrm{ord}_p(\lambda_i(s)(\lambda_i(s)-1)) = \mathrm{ord}_p(|G_i|) = 0.$$

Then

$${}_2F_1(\lambda_i(s))_p \equiv -\phi_p(-D_i(s))(1+p^{-1}) \pmod{|G_i|}.$$

Remark. If we let $i = 21$ and $s = \frac{1}{2}$ in Theorem 1 we obtain Example (1).

The Proof of Theorem 1.

We begin by recalling some basic facts about elliptic curves.

Let $E = E/\mathbb{Q}$ be the set of points (x, y) with $x, y \in \mathbb{Q}$ satisfying the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{4}$$

where $a_i \in \mathbb{Q}$. We define constants

$$\begin{aligned} b_2 &:= a_1^2 + 4a_2 \\ b_4 &:= 2a_4 + a_1a_3 \\ b_6 &:= a_3^2 + 4a_6 \\ b_8 &:= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned}$$

Replacing y by $\frac{1}{2}(y - a_1x - a_3)$ in (4) gives us

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6. \tag{5}$$

Multiplying both sides of (5) by 16 and replacing y by $y/4$ and x by $x/4$ yields

$$y^2 = x^3 + b_2x^2 + 8b_4x + 16b_6. \tag{6}$$

We also define the discriminant and j-invariant of E:

$$\begin{aligned} \Delta(E) &:= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ j(E) &:= \frac{(b_2^2 - 24b_4)^3}{\Delta(E)}. \end{aligned}$$

If $\Delta(E) \neq 0$, then E is an elliptic curve. Mordell's Theorem states that the points of an elliptic curve including the point at infinity form a finitely generated abelian group.

We say that p is a prime of good reduction for E if $\mathrm{ord}_p(\Delta(E)) = 0$. In this case, we can view the reduction of the elliptic curve E modulo p as an elliptic curve over $GF(p)$. We denote the reduction of E by E_p.

As in [O, Sec.3], we consider the family of elliptic curves

$${}_2E_1(\lambda) : y^2 = x(x-1)(x-\lambda), \tag{7}$$

where $\lambda \in \mathbb{Q} \setminus \{0, 1\}$ since

$$\Delta({}_2E_1(\lambda)) = 16\lambda^2(\lambda - 1)^2. \tag{8}$$

Note that its 2-torsion points are $\{(0, 0), (1, 0), (\lambda, 0), \infty\}$. Also, we observe that

$$j({}_2E_1(\lambda)) = \frac{256(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

If p is an odd prime such that $\text{ord}_p(\lambda(\lambda - 1)) = 0$, then p is a prime of good reduction for ${}_2E_1(\lambda)$ and we define

$${}_2a_1(p; \lambda) := p + 1 - |{}_2E_1(\lambda)_p|, \tag{9}$$

where $|{}_2E_1(\lambda)_p|$ denotes the number of $GF(p)$-points of ${}_2E_1(\lambda)_p$ including the point at infinity. Theorem 2 illustrates the significance of the elliptic curves ${}_2E_1(\lambda)$ in the study of the functions ${}_2F_1(\lambda)_p$.

Theorem 2. [O, Thm.1] *If $\lambda \in \mathbb{Q}\setminus\{0, 1\}$ and p is an odd prime for which $\text{ord}_p(\lambda(\lambda-1)) = 0$, then*

$${}_2F_1(\lambda)_p = \frac{-\phi_p(-1){}_2a_1(p; \lambda)}{p}. \tag{10}$$

The idea of a quadratic twist of an elliptic curve is particularly useful for our purposes. If E is an elliptic curve with rational coefficients having equation

$$E : y^2 = x^3 + ax^2 + bx + c,$$

and if D is a squarefree integer, then the D-quadratic twist of E is defined as

$$E(D) : y^2 = x^3 + aDx^2 + bD^2x + cD^3.$$

Moreover, if $p \geq 5$ is a prime of good reduction for E and $E(D)$, then

$$a(p) = \phi_p(D)a_D(p), \tag{11}$$

where $a(p) = p + 1 - |E_p|$ and $a_D(p) = p + 1 - |E(D)_p|$. Proposition 3 states an important property of elliptic curves which are twists of each other.

Proposition 3. [S, X. Corollary 5.4.1] *If E_1 and E_2 are quadratic twists of each other, then $j(E_1) = j(E_2)$.*

In particular, we are interested in the numbers ${}_2a_1(p; \lambda) \pmod N$ when a quadratic twist of ${}_2E_1(\lambda)$ has torsion subgroup of size N.

Proposition 4. *Suppose that $E/\mathbb{Q}$ is an elliptic curve with torsion subgroup G which is a D-quadratic twist of ${}_2E_1(\lambda)$. If $p \geq 5$ is a prime for which E has good reduction and*

$$\mathrm{ord}_p(\lambda(\lambda-1)) = \mathrm{ord}_p(|G|) = 0,$$

then

$${}_2F_1(\lambda)_p \equiv -\phi_p(-D)(1+p^{-1}) \pmod{|G|}.$$

Proof. Notice that p is a prime of good reduction for ${}_2E_1(\lambda)$ since $\mathrm{ord}_p(\lambda(\lambda-1)) = 0$. Therefore,

$$\begin{aligned} p+1-|E_p| &= a(p) \\ &= \phi_p(D)\,{}_2a_1(p;\lambda). \end{aligned}$$

Observing that the reduction map $E \to E_p$ is injective on the torsion subgroup of E since $\mathrm{ord}_p(|G|) = 0$ [S, VII. Prop.3.1(b)], we also have that

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

Hence,

$$(p+1)\phi_p(D) \equiv {}_2a_1(p;\lambda) \pmod{|G|}. \tag{12}$$

Substituting (12) in (10) proves the Proposition.

Proof of Theorem 1. We prove Theorem 1 for $i = 13$. The proofs of the other cases are very similar. In this case, $G_{13} = \mathbb{Z}2 \times \mathbb{Z}6$. Any elliptic curve $E/\mathbb{Q}$ with torsion subgroup $\mathbb{Z}2 \times \mathbb{Z}6$ may be written [Ku, Table 3]:

$$E : y^2 + (1-c)xy - by = x^3 - bx^2, \tag{13}$$

where

$$\begin{aligned} c &:= \frac{10-2s}{(s^2-9)}, \\ b &:= c + c^2, \end{aligned}$$

and $s \in \mathbb{Q} \setminus S_{13}$ since

$$\Delta(E) = \frac{64(s-1)^6(s-5)^6(s-9)^2}{(s-3)^{10}(s+3)^{10}}. \tag{14}$$

We also calculate that

$$j(E) = \frac{(s^2-6s+21)^3(s^6-18s^5+75s^4+180s^3-825s^2-2178s+6861)^3}{64(s-9)^2(s-5)^9(s-1)^6(s-3)^2(s+3)^2}.$$

Setting $j(E) = j({}_2E_1(\lambda))$ and solving for λ gives six solutions: $\{\lambda_{10}(s), ..., \lambda_{15}(s)\}$. Choosing the solution

$$\lambda_{13}(s) = \frac{128(s-3)}{(s+3)(s-5)^3},$$

we find that

$$\Delta({}_2E_1(\lambda_{13}(s))) = \frac{262144(s-1)^6(s-3)^2(s-9)^2}{(s+3)^4(s-5)^{12}}. \tag{15}$$

Thus, if $s \notin S_{13}$, then ${}_2E_1(\lambda_{13}(s))$ is an elliptic curve. Furthermore, by comparing (14) and (15) we see that the primes of bad reduction for E which are greater than or equal to 5 are also primes of bad reduction for ${}_2E_1(\lambda_{13}(s))$. Rewriting the curve (13) in the form (6) we obtain

$$E : y^2 = \left(x + \frac{8(s-5)}{(s-3)(s+3)}\right)\left(x + \frac{s^3 - 7s^2 + 11s - 5}{s^3 - 3s^2 - 9s + 27}\right)\left(x + \frac{8(s-1)^2}{s^3 + 3s^2 - 9s - 27}\right).$$

Letting $x \to x - \frac{8(s-5)}{(s-3)(s+3)}$ transforms this into

$$\begin{aligned} E : y^2 &= x(x - t_{13}(s))(x - \lambda_{13}(s)t_{13}(s)) \\ &= x^3 - (1 + \lambda_{13}(s))t_{13}(s)x^2 + \lambda_{13}(s)t_{13}(s)^2 x, \end{aligned} \tag{16}$$

where

$$t_{13}(s) := -\frac{(s-5)^3}{(s+3)(s-3)^2}.$$

Equation (16) shows that E is the $t_{13}(s)$ quadratic twist of ${}_2E_1(\lambda_{13}(s))$. We then define $D_{13}(s)$ to be the squarefree part of $t_{13}(s)$:

$$D_{13}(s) = -(s+3)(s-5),$$

and apply Proposition 4 to obtain

$${}_2F_1\left(\frac{128(s-3)}{(s+3)(s-5)^3}\right)_p \equiv -\phi_p((s+3)(s-5))(1 + p^{-1}) \pmod{12}.$$

The remaining cases of Theorem 1 follow by repeating this argument for all possible torsion subgroups containing $\mathbb{Z}2 \times \mathbb{Z}2$ (since any twist of ${}_2E_1(\lambda)$ must have full 2-torsion.) Kubert's table gives a parametrization of all curves having such torsion subgroups.

References

[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.

[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.

[O-P] K. Ono and D. Penniston, *Congruences for ${}_3F_2$ hypergeometric functions over finite fields*, Illinois Journal of Mathematics, accepted for publication.

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

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