

*Pacific
Journal of
Mathematics*

**THE TRACE OF FROBENIUS OF ELLIPTIC CURVES
AND THE p -ADIC GAMMA FUNCTION**

DERMOT MCCARTHY

Volume 261 No. 1

January 2013

THE TRACE OF FROBENIUS OF ELLIPTIC CURVES AND THE p -ADIC GAMMA FUNCTION

DERMOT MCCARTHY

We define a function in terms of quotients of the p -adic gamma function which generalizes earlier work of the author on extending hypergeometric functions over finite fields to the p -adic setting. We prove, for primes $p > 3$, that the trace of Frobenius of any elliptic curve over \mathbb{F}_p , whose j -invariant does not equal 0 or 1728, is just a special value of this function. This generalizes results of Fuselier and Lennon which evaluate the trace of Frobenius in terms of hypergeometric functions over \mathbb{F}_p when $p \equiv 1 \pmod{12}$.

1. Introduction and statement of results

Let \mathbb{F}_p denote the finite field with p , a prime, elements. Consider E/\mathbb{Q} an elliptic curve with an integral model of discriminant $\Delta(E)$. We denote E_p the reduction of E modulo p . We note that E_p is nonsingular, and hence an elliptic curve over \mathbb{F}_p , if and only if $p \nmid \Delta(E)$, in which case we say p is a prime of good reduction. Regardless, we define

$$(1-1) \quad a_p(E) := p + 1 - \#E_p(\mathbb{F}_p).$$

If p is not a prime of good reduction we know $a_p(E) = 0, \pm 1$ depending on the nature of the singularity. If p is a prime of good reduction, we refer to $a_p(E)$ as the *trace of Frobenius* as it can be interpreted as the trace of the Frobenius endomorphism of E/\mathbb{F}_p . For a given elliptic curve E/\mathbb{Q} , these a_p are important quantities. Recall the Hasse–Weil L -function of E (viewed as function of a complex variable s) is defined by

$$L(E, s) := \prod_{p|\Delta} \frac{1}{1 - a_p(E)p^{-s}} \prod_{p \nmid \Delta} \frac{1}{1 - a_p(E)p^{-s} + p^{1-2s}}.$$

This Euler product converges for $\operatorname{Re}(s) > \frac{3}{2}$ and has analytic continuation to the whole complex plane. The Birch and Swinnerton-Dyer conjecture concerns the behavior of $L(E, s)$ at $s = 1$.

MSC2010: primary 11G20, 33E50; secondary 33C99, 11S80.

Keywords: elliptic curves, p -adic gamma function, trace of Frobenius, hypergeometric functions, modular forms.

The main result of this paper relates the trace of Frobenius to a special value of a function which we define in terms of quotients of the p -adic gamma function. Let $\Gamma_p(\cdot)$ denote Morita's p -adic gamma function and let ω denote the Teichmüller character of \mathbb{F}_p with $\bar{\omega}$ denoting its character inverse. For $x \in \mathbb{Q}$ we let $\lfloor x \rfloor$ denote the greatest integer less than or equal to x and $\langle x \rangle$ the fractional part of x , i.e., $x - \lfloor x \rfloor$.

Definition 1.1. Let p be an odd prime and let $t \in \mathbb{F}_p$. For $n \in \mathbb{Z}^+$ and $1 \leq i \leq n$, let $a_i, b_i \in \mathbb{Q} \cap \mathbb{Z}_p$. Then we define

$${}_nG_n \left[\begin{matrix} a_1, a_2, \dots, a_n \\ b_1, b_2, \dots, b_n \end{matrix} \middle| t \right]_p := \frac{-1}{p-1} \sum_{j=0}^{p-2} (-1)^{jn} \bar{\omega}^j(t) \\ \times \prod_{i=1}^n \frac{\Gamma_p(\langle a_i - \frac{j}{p-1} \rangle)}{\Gamma_p(\langle a_i \rangle)} \frac{\Gamma_p(\langle -b_i + \frac{j}{p-1} \rangle)}{\Gamma_p(\langle -b_i \rangle)} (-p)^{-\lfloor \langle a_i \rangle - \frac{j}{p-1} \rfloor - \lfloor \langle -b_i \rangle + \frac{j}{p-1} \rfloor}.$$

Throughout the paper we will refer to this function as ${}_nG_n[\dots]$. The value of ${}_nG_n[\dots]$ depends only on the fractional part of the a and b parameters. Therefore, we can assume $0 \leq a_i, b_i < 1$.

This function has some very nice properties. It generalizes the function defined by the author in [McCarthy 2012a], which exhibits relationships to Fourier coefficients of modular forms. This earlier function has only one line of parameters and corresponds to ${}_nG_n[\dots]$ when all the bottom line parameters are integral and $t = 1$. The earlier function also extended, to the p -adic setting, hypergeometric functions over finite fields with trivial bottom line parameters. In Section 3 we will see that ${}_nG_n[\dots]$ extends hypergeometric functions over finite fields in their full generality, to the p -adic setting. By definition, results involving hypergeometric functions over finite fields will often be restricted to primes in certain congruence classes; see for example [Evans 2010; Fuselier 2010; Lennon 2011; Mortenson 2005; Vega 2011]. The motivation for developing ${}_nG_n[\dots]$ is that it can often allow these results to be extended to a wider class of primes [McCarthy 2012a; 2012b], as we exhibit in our main result below. We will discuss these properties in more detail in Section 3.

We now state our main result, which relates the trace of Frobenius of an elliptic curve over \mathbb{F}_p to a special value of ${}_nG_n[\dots]$. We first note that if $p > 3$ then any elliptic curve over \mathbb{F}_p is isomorphic to an elliptic curve of the form

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

that is, short Weierstrass form, and that the trace of Frobenius of isomorphic curves are equal. Let $j(E)$ denote the j -invariant of the elliptic curve E . Let $\phi_p(\cdot)$ be the Legendre symbol modulo p . We will often omit the subscript p when it is clear from the context.

Theorem 1.2. *Let $p > 3$ be prime. Consider an elliptic curve E/\mathbb{F}_p of the form $E : y^2 = x^3 + ax + b$ with $j(E) \neq 0, 1728$. Then*

$$(1-2) \quad a_p(E) = \phi(b) \cdot p \cdot {}_2G_2 \left[\begin{matrix} \frac{1}{4}, & \frac{3}{4} \\ \frac{1}{3}, & \frac{2}{3} \end{matrix} \middle| -\frac{27b^2}{4a^3} \right]_p.$$

Independent of Theorem 1.2, we will see later from Proposition 3.1 that the right-hand side of (1-2) is p -integral.

Theorem 1.2 generalizes Theorem 1.2 of [Fuselier 2010] and Theorem 2.1 of [Lennon 2011], which evaluate the trace of Frobenius in terms of hypergeometric functions over \mathbb{F}_p when $p \equiv 1 \pmod{12}$. The results in the latter paper are in fact over \mathbb{F}_q , for $q \equiv 1 \pmod{12}$ a prime power, and hence allow calculation of a_p up to sign when $p \not\equiv 1 \pmod{12}$ via the relation $a_p^2 = a_{p^2} + 2p$. Theorem 1.2 however gives a direct evaluation of a_p for all primes $p > 3$ and resolves this sign issue.

One of the nice features of the main result in [Lennon 2011] is that it is independent of the Weierstrass model of the elliptic curve. Recall an elliptic curve over a field \mathbb{K} in Weierstrass form is given by

$$(1-3) \quad E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with $a_1, a_2, \dots, a_6 \in \mathbb{K}$. We can define the quantities

$$\begin{aligned} b_2 &:= a_1^2 + 4a_2, & b_4 &:= 2a_4 + a_1a_3, & b_6 &:= a_3^2 + 4a_6, \\ b_8 &:= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, & c_4 &:= b_2^2 - 24b_4, \\ c_6 &:= -b_2^3 + 36b_2b_4 - 216b_6, \end{aligned}$$

in the standard way. These can then be used to calculate $\Delta(E) = (c_4^3 - c_6^2)/1728$ and $j(E) = c_4^3/\Delta(E)$. An admissible change of variables, $x = u^2x' + r$ and $y = u^3y' + su^2x' + t$ with $u, r, s, t, \in \mathbb{K}$ and $u \neq 0$ in (1-3) will result in an isomorphic curve also given in Weierstrass form, and any two isomorphic curves over \mathbb{K} are related by such an admissible change of variables. Two curves related by an admissible change of variables will have the same j -invariant but their discriminants will differ by a factor of a twelfth-power, namely u^{12} , and their respective c_i quantities will differ by a factor of u^i . This allows the main result [ibid.], which is stated in terms of $j(E)$ and $\Delta(E)$, to be expressed independently of the Weierstrass model of the elliptic curve. We can do something similar with Theorem 1.2.

Corollary 1.3. *Let $p > 3$ be prime. Consider an elliptic curve E/\mathbb{F}_p in Weierstrass form with $j(E) \neq 0, 1728$. Then*

$$a_p(E) = \phi(-6 \cdot c_6) \cdot p \cdot {}_2G_2 \left[\begin{matrix} \frac{1}{4}, & \frac{3}{4} \\ \frac{1}{3}, & \frac{2}{3} \end{matrix} \middle| 1 - \frac{1728}{j(E)} \right]_p.$$

Please refer to [Knapp 1992; Silverman 2009] for a detailed account of any of the properties of elliptic curves mentioned in the above discussion. The rest of this paper is organized as follows. In Section 2 we recall some basic properties of multiplicative characters, Gauss sums and the p -adic gamma function. We discuss some properties of ${}_nG_n[\dots]$ in Section 3, including its relationship to hypergeometric functions over finite fields. The proofs of our main results are contained in Section 4. Finally, we make some closing remarks in Section 5.

2. Preliminaries

Let \mathbb{Z}_p denote the ring of p -adic integers, \mathbb{Q}_p the field of p -adic numbers, $\overline{\mathbb{Q}}_p$ the algebraic closure of \mathbb{Q}_p , and \mathbb{C}_p the completion of $\overline{\mathbb{Q}}_p$.

2A. Multiplicative characters and Gauss sums. Let $\widehat{\mathbb{F}}_p^*$ denote the group of multiplicative characters of \mathbb{F}_p^* . We extend the domain of $\chi \in \widehat{\mathbb{F}}_p^*$ to \mathbb{F}_p , by defining $\chi(0) := 0$ (including the trivial character ε) and denote by $\bar{\chi}$ the inverse of χ . We recall the following orthogonal relations. For $\chi \in \widehat{\mathbb{F}}_p^*$ we have

$$(2-1) \quad \sum_{x \in \mathbb{F}_p} \chi(x) = \begin{cases} p-1 & \text{if } \chi = \varepsilon, \\ 0 & \text{if } \chi \neq \varepsilon, \end{cases}$$

and, for $x \in \mathbb{F}_p$ we have

$$(2-2) \quad \sum_{\chi \in \widehat{\mathbb{F}}_p^*} \chi(x) = \begin{cases} p-1 & \text{if } x = 1, \\ 0 & \text{if } x \neq 1. \end{cases}$$

We now introduce some properties of Gauss sums. For further details see [Berndt et al. 1998], noting that we have adjusted results to take into account $\varepsilon(0) = 0$.

Let ζ_p be a fixed primitive p -th root of unity in $\overline{\mathbb{Q}}_p$. We define the additive character $\theta : \mathbb{F}_p \rightarrow \mathbb{Q}_p(\zeta_p)$ by $\theta(x) := \zeta_p^x$. It is easy to see that

$$(2-3) \quad \theta(a + b) = \theta(a)\theta(b),$$

$$(2-4) \quad \sum_{x \in \mathbb{F}_p} \theta(x) = 0.$$

We note that \mathbb{Q}_p contains all $(p - 1)$ -th roots of unity and in fact they are all in \mathbb{Z}_p^* . Thus we can consider multiplicative characters of \mathbb{F}_p^* to be maps $\chi : \mathbb{F}_p^* \rightarrow \mathbb{Z}_p^*$. Recall then that for $\chi \in \widehat{\mathbb{F}}_p^*$, the Gauss sum $g(\chi)$ is defined by $g(\chi) := \sum_{x \in \mathbb{F}_p} \chi(x)\theta(x)$. It easily follows from (2-2) that we can express the additive character as a sum of Gauss sums. Specifically, for $x \in \mathbb{F}_p^*$ we have

$$(2-5) \quad \theta(x) = \frac{1}{p-1} \sum_{\chi \in \widehat{\mathbb{F}}_p^*} g(\bar{\chi}) \chi(x).$$

The following important result gives a simple expression for the product of two Gauss sums. For $\chi \in \widehat{\mathbb{F}_p^*}$ we have

$$(2-6) \quad g(\chi)g(\bar{\chi}) = \begin{cases} \chi(-1)p & \text{if } \chi \neq \varepsilon, \\ 1 & \text{if } \chi = \varepsilon. \end{cases}$$

Another important product formula for Gauss sums is the Hasse–Davenport formula.

Theorem 2.1 (Hasse, Davenport [Berndt et al. 1998, Theorem 11.3.5]). *Let χ be a character of order m of \mathbb{F}_p^* for some positive integer m . For a character ψ of \mathbb{F}_p^* we have*

$$\prod_{i=0}^{m-1} g(\chi^i \psi) = g(\psi^m) \psi^{-m}(m) \prod_{i=1}^{m-1} g(\chi^i).$$

We now recall a formula for counting zeros of polynomials in affine space using the additive character. If $f(x_1, x_2, \dots, x_n) \in \mathbb{F}_p[x_1, x_2, \dots, x_n]$, then the number of points, N_p , in $\mathbb{A}^n(\mathbb{F}_p)$ satisfying $f(x_1, x_2, \dots, x_n) = 0$ is given by

$$(2-7) \quad pN_p = p^n + \sum_{y \in \mathbb{F}_p^*} \sum_{x_1, x_2, \dots, x_n \in \mathbb{F}_p} \theta(y f(x_1, x_2, \dots, x_n)).$$

2B. p -adic preliminaries. We define the Teichmüller character to be the primitive character $\omega : \mathbb{F}_p \rightarrow \mathbb{Z}_p^*$ satisfying $\omega(x) \equiv x \pmod{p}$ for all $x \in \{0, 1, \dots, p-1\}$. We now recall the p -adic gamma function. For further details, see [Koblitz 1980]. Let p be an odd prime. For $n \in \mathbb{Z}^+$ we define the p -adic gamma function as

$$\Gamma_p(n) := (-1)^n \prod_{\substack{0 < j < n \\ p \nmid j}} j,$$

and extend to all $x \in \mathbb{Z}_p$ by setting $\Gamma_p(0) := 1$ and

$$\Gamma_p(x) := \lim_{n \rightarrow x} \Gamma_p(n)$$

for $x \neq 0$, where n runs through any sequence of positive integers p -adically approaching x . This limit exists, is independent of how n approaches x , and determines a continuous function on \mathbb{Z}_p with values in \mathbb{Z}_p^* . We now state a product formula for the p -adic gamma function. If $m \in \mathbb{Z}^+$, $p \nmid m$ and $x = r/(p-1)$ with $0 \leq r \leq p-1$ then

$$(2-8) \quad \prod_{h=0}^{m-1} \Gamma_p\left(\frac{x+h}{m}\right) = \omega(m^{(1-x)(1-p)}) \Gamma_p(x) \prod_{h=1}^{m-1} \Gamma_p\left(\frac{h}{m}\right).$$

We note also that

$$(2-9) \quad \Gamma_p(x) \Gamma_p(1-x) = (-1)^{x_0},$$

where $x_0 \in \{1, 2, \dots, p\}$ satisfies $x_0 \equiv x \pmod{p}$. The Gross–Koblitz formula [1979] allows us to relate Gauss sums and the p -adic gamma function. Let $\pi \in \mathbb{C}_p$ be the fixed root of $x^{p-1} + p = 0$ which satisfies $\pi \equiv \zeta_p - 1 \pmod{(\zeta_p - 1)^2}$. Then we have the following result.

Theorem 2.2 [Gross and Koblitz 1979]. *For $j \in \mathbb{Z}$,*

$$g(\bar{\omega}^j) = -\pi^{(p-1)\langle \frac{j}{p-1} \rangle} \Gamma_p\left(\left\langle \frac{j}{p-1} \right\rangle\right).$$

3. Properties of ${}_nG_n[\dots]$.

As both $\Gamma_p(\cdot)$ and $\omega(\cdot)$ are in \mathbb{Z}_p^* , we see immediately from its definition that ${}_nG_n[\dots]_p \in p^\delta \mathbb{Z}_p$ for some $\delta \in \mathbb{Z}$. We describe δ explicitly in the following proposition. We first define

$$\langle b_i \rangle^* := 1 - \langle -b_i \rangle = \begin{cases} \langle b_i \rangle & \text{if } b_i \notin \mathbb{Z}, \\ 1 & \text{if } b_i \in \mathbb{Z}. \end{cases}$$

Proposition 3.1. *Let p be an odd prime and let $t \in \mathbb{F}_p$. Let $n \in \mathbb{Z}^+$, $1 \leq i \leq n$ and $a_i, b_i \in \mathbb{Q} \cap \mathbb{Z}_p$. For $j \in \mathbb{Z}$ we define*

$$f(j) := \#\{a_i \mid \langle a_i \rangle < \frac{j}{p-1}, 1 \leq i \leq n\} - \#\{b_i \mid \langle b_i \rangle^* \leq \frac{j}{p-1}, 1 \leq i \leq n\}.$$

Then

$${}_nG_n\left[\begin{matrix} a_1, & a_2, & \dots, & a_n \\ b_1, & b_2, & \dots, & b_n \end{matrix} \middle| t\right]_p \in p^\delta \mathbb{Z}_p,$$

where $\delta = \text{Min}\{f(j) \mid 0 \leq j \leq p-2\}$.

Proof. As $\Gamma_p(\cdot)$, $\omega(\cdot)$ and $\frac{1}{p-1}$ are all in \mathbb{Z}_p^* , the result follows from noting that

$$\lfloor \langle a_i \rangle - \frac{j}{p-1} \rfloor = \begin{cases} -1 & \text{if } \langle a_i \rangle < j/(p-1), \\ 0 & \text{if } \langle a_i \rangle \geq j/(p-1), \end{cases}$$

and

$$\lfloor \langle -b_i \rangle + \frac{j}{p-1} \rfloor = \begin{cases} 1 & \text{if } \langle b_i \rangle^* \leq j/(p-1), \\ 0 & \text{if } \langle b_i \rangle^* > j/(p-1). \end{cases} \quad \square$$

We note that ${}_nG_n[\dots]$ generalizes the function defined in [McCarthy 2012a]. This earlier function has only one line of parameters and corresponds to ${}_nG_n[\dots]$ when all the bottom line parameters are integral and $t = 1$. Therefore the results from [McCarthy 2012a; 2012b] can be restated using ${}_nG_n[\dots]$. The motivation for developing ${}_nG_n[\dots]$ and its predecessor was to allow results involving hypergeometric functions over finite fields, which are often restricted to primes in certain congruence classes, to be extended to a wider class of primes. While the function defined in [McCarthy 2012a] extended to the p -adic setting, hypergeometric functions over

finite fields with trivial bottom line parameters, we now show, in Lemma 3.3, that ${}_nG_n[\dots]$ extends hypergeometric functions over finite fields in their full generality.

Hypergeometric functions over finite fields were originally defined by Greene [1987], who first established these functions as analogues of classical hypergeometric functions. Functions of this type were also introduced by Katz [1990] about the same time. In the present article we use a normalized version of these functions defined in [McCarthy 2012c], which is more suitable for our purposes. The reader is directed to [ibid., §2] for the precise connections among these three classes of functions.

Definition 3.2 [McCarthy 2012c, Definition 1.4]. For $A_0, A_1, \dots, A_n, B_1, \dots, B_n$ in $\widehat{\mathbb{F}}_p^*$ and x in \mathbb{F}_p , define

$$(3-1) \quad {}_{n+1}F_n \left(\begin{matrix} A_0, & A_1, & \dots, & A_n \\ & B_1, & \dots, & B_n \end{matrix} \middle| x \right)_p \\ := \frac{1}{p-1} \sum_{\chi \in \widehat{\mathbb{F}}_p^*} \prod_{i=0}^n \frac{g(A_i \chi)}{g(A_i)} \prod_{j=1}^n \frac{g(\overline{B_j \chi})}{g(\overline{B_j})} g(\overline{\chi}) \chi(-1)^{n+1} \chi(x).$$

Many of the results concerning hypergeometric functions over finite fields that we quote from other articles were originally stated using Greene's function. If this is the case, note then that we have reformulated them in terms ${}_{n+1}F_n(\dots)$ as defined above.

We have the following relationship between ${}_nG_n[\dots]$ and ${}_{n+1}F_n(\dots)$.

Lemma 3.3. For a fixed odd prime p , let $A_i, B_k \in \widehat{\mathbb{F}}_p^*$ be given by $\overline{\omega}^{a_i(p-1)}$ and $\overline{\omega}^{b_k(p-1)}$ respectively, where ω is the Teichmüller character. Then

$${}_{n+1}F_n \left(\begin{matrix} A_0, & A_1, & \dots, & A_n \\ & B_1, & \dots, & B_n \end{matrix} \middle| t \right)_p = {}_{n+1}G_{n+1} \left[\begin{matrix} a_0, & a_1, & \dots, & a_n \\ 0, & b_1, & \dots, & b_n \end{matrix} \middle| t^{-1} \right]_p.$$

Proof. Starting from the definition of ${}_{n+1}F_n(\dots)$, we convert the right-hand side of (3-1) to an expression involving the p -adic gamma function and Teichmüller character. We note $\widehat{\mathbb{F}}_p^*$ can be given by $\{\omega^j \mid 0 \leq j \leq p-2\}$. Then, straightforward applications of the Gross–Koblitz formula (Theorem 2.2) with $\chi = \omega^j$ yield

$$g(\overline{\chi}) = -\pi^j \Gamma_p \left(\frac{j}{p-1} \right), \\ \frac{g(A_i \chi)}{g(A_i)} = \pi^{-j-(p-1)} (\lfloor a_i - \frac{j}{p-1} \rfloor - \lfloor a_i \rfloor) \frac{\Gamma_p(\langle a_i - \frac{j}{p-1} \rangle)}{\Gamma_p(\langle a_i \rangle)}, \\ \frac{g(\overline{B_k \chi})}{g(\overline{B_k})} = \pi^{j-(p-1)} (\lfloor -b_k + \frac{j}{p-1} \rfloor - \lfloor -b_k \rfloor) \frac{\Gamma_p(\langle -b_k + \frac{j}{p-1} \rangle)}{\Gamma_p(\langle -b_k \rangle)},$$

where π is as defined in Section 2B. Substituting these expressions into (3-1) and tidying up yields the result. \square

We note that if $\chi \in \widehat{\mathbb{F}}_p^*$ is a character of order d and is given by $\overline{\omega}^x(p-1)$ then $x = m/d \in \mathbb{Q}$ and $p \equiv 1 \pmod{d}$. Therefore, given a hypergeometric function over \mathbb{F}_p whose arguments are characters of prescribed order, the function will only be defined for primes p in certain congruence classes. By Lemma 3.3, for primes in these congruence classes, the finite field hypergeometric function will be related to an appropriate ${}_nG_n[\dots]$ function. However this corresponding ${}_nG_n[\dots]$ will be defined at all primes not dividing the orders of the particular characters appearing in the finite field hypergeometric function. This opens the possibility of extending results involving hypergeometric functions over finite fields to all but finitely many primes.

For example, we have the following result from [McCarthy 2012b], which relates a special value of the hypergeometric function over finite fields to a p -th Fourier coefficient of a certain modular form. Let

$$(3-2) \quad f(z) := f_1(z) + 5f_2(z) + 20f_3(z) + 25f_4(z) + 25f_5(z) = \sum_{n=1}^{\infty} c(n)q^n,$$

where $f_i(z) := \eta^{5-i}(z)\eta^4(5z)\eta^{i-1}(25z)$, $\eta(z) := q^{1/24} \prod_{n=1}^{\infty} (1 - q^n)$ is the Dedekind eta function and $q := e^{2\pi iz}$. Then f is a cusp form of weight four on the congruence subgroup $\Gamma_0(25)$.

Theorem 3.4 [McCarthy 2012b, Corollary 1.6]. *If $p \equiv 1 \pmod{5}$ is prime, $\chi_5 \in \widehat{\mathbb{F}}_p^*$ is a character of order 5 and $c(p)$ is as defined in (3-2), then*

$${}_4F_3 \left(\begin{matrix} \chi_5, & \chi_5^2, & \chi_5^3, & \chi_5^4 \\ \varepsilon, & \varepsilon, & \varepsilon & \end{matrix} \middle| 1 \right)_p - p = c(p).$$

This result can be extended to almost all primes using ${}_nG_n[\dots]$, as follows.

Theorem 3.5 [McCarthy 2012b, Theorem 1.4]. *If $p \neq 5$ is an odd prime and $c(p)$ is as defined in (3-2), then*

$${}_4G_4 \left[\begin{matrix} \frac{1}{5}, & \frac{2}{5}, & \frac{3}{5}, & \frac{4}{5} \\ 0, & 0, & 0, & 0 \end{matrix} \middle| 1 \right]_p - \left(\frac{5}{p}\right)p = c(p),$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol modulo p .

Results in [Mortenson 2005] establish congruences modulo p^2 between the classical hypergeometric series and the hypergeometric function over \mathbb{F}_p , for primes p in certain congruence classes. In [McCarthy 2012a] we extend these results to primes in additional congruence classes and, in some cases to modulo p^3 , using the predecessor to ${}_nG_n[\dots]$.

The main purpose of this paper is to extend to almost all primes the results in [Lennon 2011], which relate the trace of Frobenius a_p to a special value of a hypergeometric function over \mathbb{F}_p when $p \equiv 1 \pmod{12}$. In addition to their formal statement, the results in [ibid.] appear in various forms throughout that paper, all of which are related by known transformations for hypergeometric function over finite fields. We recall one such version of [ibid., Theorem 2.1].

Theorem 3.6 [Lennon 2011, §2.2]. *Let $p \equiv 1 \pmod{12}$ be prime and let $\psi \in \widehat{\mathbb{F}}_p^*$ be a character of order 12. Consider an elliptic curve E/\mathbb{F}_p of the form*

$$E : y^2 = x^3 + ax + b$$

with $j(E) \neq 0, 1728$. Then

$$a_p(E) = \psi^3 \left(-\frac{a^3}{27} \right) \cdot {}_2F_1 \left(\psi, \psi^5 \mid \frac{4a^3 + 27b^2}{4a^3} \right)_p.$$

Theorem 3.6 generalizes [Fuselier 2010, Theorem 1.2] and other results from Fuselier's thesis [2007] that provide similar results for various families of elliptic curves. In attempting to extend Theorem 3.6 beyond $p \equiv 1 \pmod{12}$, one might consider using

$${}_2G_2 \left[\begin{matrix} \frac{1}{12}, \frac{5}{12} \\ 0, 0 \end{matrix} \mid \frac{4a^3}{4a^3 + 27b^2} \right]_p,$$

as suggested by Lemma 3.3. However this leads to poor results when $p \not\equiv 1 \pmod{12}$. Results where ${}_nG_n[\dots]$ extend those involving ${}_{n+1}F_n(\dots)$ seem to work best when the arguments of ${}_nG_n[\dots]$ appear in sets such that for each denominator all possible relatively prime numerators are represented. This is reflected in Theorem 1.2.

Hypergeometric functions over finite fields have been applied to many areas but most interestingly perhaps has been their relationships to modular forms [Ahlgren and Ono 2000; Evans 2010; Fuselier 2010; Frechette et al. 2004; McCarthy 2012b; Mortenson 2005; Ono 1998; Papanikolas 2006] and their use in evaluating the number of points over \mathbb{F}_p on certain algebraic varieties [Ahlgren and Ono 2000; Fuselier 2010; McCarthy 2012b; Vega 2011]. Lemma 3.3 allows these results to be expressed in terms of ${}_nG_n[\dots]$ also. Many of these cited results are based on ${}_{n+1}F_n(\dots)$ with arguments which are characters of order at most 2 and hold for all odd primes. However there is much scope for developing results where the characters involved have higher orders, in which case these functions will be defined for primes in certain congruence classes and ${}_nG_n[\dots]$ allows the possibility to extend these results to a wider class of primes.

4. Proofs of Theorem 1.2 and Corollary 1.3

We first prove a preliminary result which we will require later for the proof of our main result.

Lemma 4.1. *Let p be prime. For $0 \leq j \leq p-2$ and $t \in \mathbb{Z}^+$ with $p \nmid t$, we have*

$$(4-1) \quad \Gamma_p\left(\left(\frac{tj}{p-1}\right)\right)\omega(t^{tj}) \prod_{h=1}^{t-1} \Gamma_p\left(\frac{h}{t}\right) = \prod_{h=0}^{t-1} \Gamma_p\left(\left(\frac{h}{t} + \frac{j}{p-1}\right)\right)$$

and

$$(4-2) \quad \Gamma_p\left(\left(\frac{-tj}{p-1}\right)\right)\omega(t^{-tj}) \prod_{h=1}^{t-1} \Gamma_p\left(\frac{h}{t}\right) = \prod_{h=0}^{t-1} \Gamma_p\left(\left(\frac{1+h}{t} - \frac{j}{p-1}\right)\right).$$

Proof. Fix $0 \leq j \leq p-2$ and let $k \in \mathbb{Z}_{\geq 0}$ be defined such that

$$(4-3) \quad k\left(\frac{p-1}{t}\right) \leq j < (k+1)\left(\frac{p-1}{t}\right).$$

Letting $m = t$ and $x = (tj/(p-1)) - k$ in (2-8) yields

$$(4-4) \quad \prod_{h=0}^{t-1} \Gamma_p\left(\frac{j}{p-1} + \frac{h-k}{t}\right) = \omega\left(t^{(1-\frac{tj}{p-1}+k)(1-p)}\right) \Gamma_p\left(\frac{tj}{p-1} - k\right) \prod_{h=1}^{t-1} \Gamma_p\left(\frac{h}{t}\right).$$

We note that $0 \leq k < t$. Using (4-3) we see that if $0 \leq h < t$ then

$$0 \leq \frac{h-k}{t} + \frac{j}{p-1} < 1.$$

Therefore, if $1 \leq k < t$ then

$$(4-5) \quad \begin{aligned} \prod_{h=0}^{t-1} \Gamma_p\left(\frac{h-k}{t} + \frac{j}{p-1}\right) &= \prod_{h=0}^{t-1} \Gamma_p\left(\left(\frac{h-k}{t} + \frac{j}{p-1}\right)\right) \\ &= \prod_{h=0}^{k-1} \Gamma_p\left(\left(\frac{t+h-k}{t} + \frac{j}{p-1}\right)\right) \prod_{h=k}^{t-1} \Gamma_p\left(\left(\frac{h-k}{t} + \frac{j}{p-1}\right)\right) \\ &= \prod_{h=t-k}^{t-1} \Gamma_p\left(\left(\frac{h}{t} + \frac{j}{p-1}\right)\right) \prod_{h=0}^{t-k-1} \Gamma_p\left(\left(\frac{h}{t} + \frac{j}{p-1}\right)\right) \\ &= \prod_{h=0}^{t-1} \Gamma_p\left(\left(\frac{h}{t} + \frac{j}{p-1}\right)\right). \end{aligned}$$

The result in (4-5) also holds when $k = 0$. Substituting (4-5) into (4-4) and noting that

$$\Gamma_p\left(\left(\frac{tj}{p-1}\right)\right) = \Gamma_p\left(\frac{tj}{p-1} - k\right),$$

by (4-3), yields (4-1).

We use a similar argument to prove (4-2). The result is trivial for $j = 0$. Fix $0 < j \leq p - 2$ and let $k \in \mathbb{Z}^+$ be defined such that

$$(4-6) \quad (k - 1)\left(\frac{p-1}{t}\right) < j \leq k\left(\frac{p-1}{t}\right).$$

Letting $m = t$ and $x = k - tj/(p - 1)$ in (2-8) yields

$$(4-7) \quad \prod_{h=0}^{t-1} \Gamma_p\left(\frac{k+h}{t} - \frac{tj}{p-1}\right) = \omega\left(t^{(1-k+\frac{tj}{p-1})(1-p)}\right) \Gamma_p\left(k - \frac{tj}{p-1}\right) \prod_{h=1}^{t-1} \Gamma_p\left(\frac{h}{t}\right).$$

We note that $1 \leq k \leq t$. Using (4-6) we see that if $0 \leq h < t$ then

$$0 \leq \frac{k+h}{t} - \frac{j}{p-1} < 1.$$

Therefore, if $1 < k \leq t$ then

$$(4-8) \quad \begin{aligned} & \prod_{h=0}^{t-1} \Gamma_p\left(\frac{k+h}{t} - \frac{j}{p-1}\right) \\ &= \prod_{h=0}^{t-1} \Gamma_p\left(\left(\frac{k+h}{t} - \frac{j}{p-1}\right)\right) \\ &= \prod_{h=0}^{t-k} \Gamma_p\left(\left(\frac{k+h}{t} - \frac{j}{p-1}\right)\right) \prod_{h=t-k+1}^{t-1} \Gamma_p\left(\left(\frac{k+h-t}{t} - \frac{j}{p-1}\right)\right) \\ &= \prod_{h=k-1}^{t-1} \Gamma_p\left(\left(\frac{1+h}{t} - \frac{j}{p-1}\right)\right) \prod_{h=0}^{k-2} \Gamma_p\left(\left(\frac{1+h}{t} - \frac{j}{p-1}\right)\right) \\ &= \prod_{h=0}^{t-1} \Gamma_p\left(\left(\frac{1+h}{t} - \frac{j}{p-1}\right)\right). \end{aligned}$$

The result in (4-8) also holds when $k = 1$. Now (4-2) follows by substituting (4-8) into (4-7) and noting that, by (4-6),

$$\Gamma_p\left(\left(\frac{-tj}{p-1}\right)\right) = \Gamma_p\left(\frac{-tj}{p-1} + k\right). \quad \square$$

Proof of Theorem 1.2. We note that $a \neq 0, b \neq 0$ and $-27b^2/(4a^3) \neq 1$ as $j(E) \neq 0, 1728$. Initially the proof proceeds along similar lines to the proofs of [Fuselier 2010, Theorem 1.2; Lennon 2011, Theorem 2.1] by using (2-7) to evaluate $\#E(\mathbb{F}_p)$. However we then transfer to the p -adic setting using the Gross–Koblitz formula (Theorem 2.2) and use properties of the p -adic gamma function, including

Lemma 4.1, to prove the desired result. By (2-7) we have

$$\begin{aligned}
 (4-9) \quad & p(\#E(\mathbb{F}_p) - 1) \\
 &= p^2 + \sum_{y \in \mathbb{F}_p^*} \sum_{x_1, x_2 \in \mathbb{F}_p} \theta(y(x_1^3 + ax_1 + b - x_2^2)) \\
 &= p^2 + \sum_{y \in \mathbb{F}_p^*} \theta(yb) + \sum_{y, x_2 \in \mathbb{F}_p^*} \theta(yb - yx_2^2) + \sum_{y, x_1 \in \mathbb{F}_p^*} \theta(yx_1^3 + ayx_1 + yb) \\
 &\quad + \sum_{y, x_1, x_2 \in \mathbb{F}_p^*} \theta(yx_1^3 + ayx_1 + by - yx_2^2).
 \end{aligned}$$

We now examine each sum of (4-9) in turn and will refer to them as S_1 to S_4 , respectively. Using (2-4) we see that

$$S_1 = \sum_{y \in \mathbb{F}_p^*} \theta(yb) = -1.$$

We use (2-3) and (2-5) to expand the remaining terms as expressions in Gauss sums. This exercise has also been carried out in the proof of [Lennon 2011, Theorem 2.1] so we only give a brief account here. Let T be a fixed generator for the group of characters of \mathbb{F}_p^* . Then

$$\begin{aligned}
 S_2 &= \sum_{y, x_2 \in \mathbb{F}_p^*} \theta(yb - yx_2^2) \\
 &= \frac{1}{(p-1)^2} \sum_{r, s=0}^{p-2} g(T^{-r})g(T^{-s})T^r(b) T^s(-1) \sum_{x_2 \in \mathbb{F}_p^*} T^{2s}(x_2) \sum_{y \in \mathbb{F}_p^*} T^{r+s}(y).
 \end{aligned}$$

We now apply (2-1) to the last summation on the right, which yields $(p-1)$ if $r = -s$ and zero otherwise. So

$$S_2 = \frac{1}{(p-1)} \sum_{s=0}^{p-2} g(T^s)g(T^{-s})T^{-s}(b)T^s(-1) \sum_{x_2 \in \mathbb{F}_p^*} T^{2s}(x_2).$$

Again we apply (2-1) to the last summation on the right, which yields $(p-1)$ if $s = 0$ or $s = (p-1)/2$, and zero otherwise. Thus, and using (2-6), we get that

$$S_2 = g(\varepsilon)g(\varepsilon) + g(\phi)g(\phi)\phi(-b) = 1 + p\phi(b).$$

Similarly,

$$\begin{aligned}
 S_3 &= \sum_{y, x_1 \in \mathbb{F}_p^*} \theta(yx_1^3 + ayx_1 + yb) \\
 &= \frac{1}{(p-1)^3} \sum_{r, s, t=0}^{p-2} g(T^{-r})g(T^{-s})g(T^{-t})T^s(a)T^t(b) \\
 &\quad \cdot \sum_{x_1 \in \mathbb{F}_p^*} T^{3r+s}(x_1) \sum_{y \in \mathbb{F}_p^*} T^{r+s+t}(y), \\
 S_4 &= \sum_{y, x_1, x_2 \in \mathbb{F}_p^*} \theta(yx_1^3 + ayx_1 + by - yx_2^2) \\
 &= \frac{1}{(p-1)^4} \sum_{j, r, s, t=0}^{p-2} g(T^{-j})g(T^{-r})g(T^{-s})g(T^{-t})T^r(a)T^s(b)T^t(-1) \\
 &\quad \cdot \sum_{x_1 \in \mathbb{F}_p^*} T^{3j+r}(x_1) \sum_{y \in \mathbb{F}_p^*} T^{j+r+s+t}(y) \sum_{x_2 \in \mathbb{F}_p^*} T^{2t}(x_2).
 \end{aligned}$$

We now apply (2-1) to the last summation on the right of S_4 , which yields $p-1$ if $t=0$ or $t=(p-1)/2$ and zero otherwise. In the case $t=0$ we find that

$$S_{4,t=0} = -S_3.$$

When $t=(p-1)/2$ we get, after applying (2-1) twice more,

$$S_{4,t=\frac{p-1}{2}} = \frac{\phi(-b)}{(p-1)} \sum_{j=0}^{p-2} g(T^{-j})g(T^{\frac{p-1}{2}-2j})g(T^{3j})g(T^{\frac{p-1}{2}})T^{-3j}(a)T^{2j}(b).$$

Combining (1-1), (4-9) and the evaluations of S_1, S_2, S_3 and S_4 we find that

$$\begin{aligned}
 (4-10) \quad a_p(E) &= -\frac{\phi(b)p}{(p-1)} \\
 &\quad - \frac{\phi(-b)}{p(p-1)} \sum_{j=1}^{p-2} g(T^{-j})g(T^{\frac{p-1}{2}-2j})g(T^{3j})g(T^{\frac{p-1}{2}})T^j\left(\frac{b^2}{a^3}\right).
 \end{aligned}$$

We know from Theorem 2.1 with $\chi = \phi = T^{\frac{p-1}{2}}$ and $\psi = T^{-2j}$ that

$$(4-11) \quad g(T^{\frac{p-1}{2}-2j}) = \frac{g(T^{-4j})g(T^{\frac{p-1}{2}})T^{4j}(2)}{g(T^{-2j})}.$$

Accounting for (4-11) in (4-10) and applying (2-6) with $\chi = \phi = T^{\frac{p-1}{2}}$ gives us

$$(4-12) \quad a_p(E) = \frac{-\phi(b)p}{(p-1)} \left[1 + \frac{1}{p} \sum_{j=1}^{p-2} \frac{g(T^{-j})g(T^{3j})g(T^{-4j})}{g(T^{-2j})} T^j \left(\frac{16b^2}{a^3} \right) \right].$$

We now take T to be the inverse of the Teichmüller character, that is, $T = \bar{\omega}$, and use the Gross–Koblitz formula (Theorem 2.2) to convert (4-12) to an expression involving the p -adic gamma function. This yields

$$(4-13) \quad a_p(E) = \frac{-\phi(b)p}{(p-1)} \left[1 - \sum_{j=1}^{p-2} (-p) \left(\lfloor \frac{-2j}{p-1} \rfloor - \lfloor \frac{-j}{p-1} \rfloor - \lfloor \frac{3j}{p-1} \rfloor - \lfloor \frac{-4j}{p-1} \rfloor - 1 \right) \cdot \frac{\Gamma_p\left(\left(\frac{-j}{p-1}\right)\right)\Gamma_p\left(\left(\frac{3j}{p-1}\right)\right)\Gamma_p\left(\left(\frac{-4j}{p-1}\right)\right)}{\Gamma_p\left(\left(\frac{-2j}{p-1}\right)\right)} \bar{\omega}^j \left(\frac{16b^2}{a^3} \right) \right].$$

Next we use Lemma 4.1 to transform the components of (4-13) which involve the p -adic gamma function. After some tidying up we then get

$$a_p(E) = \frac{-\phi(b)p}{(p-1)} \left[1 - \sum_{j=1}^{p-2} (-p) \left(\lfloor \frac{-2j}{p-1} \rfloor - \lfloor \frac{-j}{p-1} \rfloor - \lfloor \frac{3j}{p-1} \rfloor - \lfloor \frac{-4j}{p-1} \rfloor - 1 \right) \Gamma_p\left(1 - \frac{j}{p-1}\right) \cdot \frac{\Gamma_p\left(\left(\frac{j}{p-1}\right)\right)\Gamma_p\left(\left(\frac{1}{4} - \frac{j}{p-1}\right)\right)\Gamma_p\left(\left(\frac{3}{4} - \frac{j}{p-1}\right)\right)\Gamma_p\left(\left(\frac{1}{3} + \frac{j}{p-1}\right)\right)\Gamma_p\left(\left(\frac{2}{3} + \frac{j}{p-1}\right)\right)}{\Gamma_p\left(\frac{1}{4}\right)\Gamma_p\left(\frac{3}{4}\right)\Gamma_p\left(\frac{1}{3}\right)\Gamma_p\left(\frac{2}{3}\right)} \bar{\omega}^j \left(\frac{27b^2}{4a^3} \right) \right].$$

We note for $0 \leq j \leq p-2$,

$$\lfloor \frac{-4j}{p-1} \rfloor - \lfloor \frac{-2j}{p-1} \rfloor = \lfloor \frac{1}{4} - \frac{j}{p-1} \rfloor + \lfloor \frac{3}{4} - \frac{j}{p-1} \rfloor,$$

and when $1 \leq j \leq p-2$,

$$\lfloor \frac{-j}{p-1} \rfloor + \lfloor \frac{3j}{p-1} \rfloor + 1 = \lfloor \frac{1}{3} + \frac{j}{p-1} \rfloor + \lfloor \frac{2}{3} + \frac{j}{p-1} \rfloor.$$

Also, by (2-9) we have, for $0 \leq j \leq p-1$,

$$\Gamma_p\left(1 - \frac{j}{p-1}\right)\Gamma_p\left(\frac{j}{p-1}\right) = (-1)^{p-j} = (-1)^p \bar{\omega}^j(-1).$$

Therefore

$$\begin{aligned}
 a_p(E) &= \frac{-\phi(b)p}{(p-1)} \left[\sum_{j=0}^{p-2} (-p)^{\left(-\lfloor \frac{1}{4} - \frac{j}{p-1} \rfloor - \lfloor \frac{3}{4} - \frac{j}{p-1} \rfloor - \lfloor \frac{1}{3} + \frac{j}{p-1} \rfloor - \lfloor \frac{2}{3} + \frac{j}{p-1} \rfloor\right)} \right. \\
 &\quad \cdot \frac{\Gamma_p\left(\left(\frac{1}{4} - \frac{j}{p-1}\right)\right) \Gamma_p\left(\left(\frac{3}{4} - \frac{j}{p-1}\right)\right)}{\Gamma_p\left(\frac{1}{4}\right) \Gamma_p\left(\frac{3}{4}\right)} \\
 &\quad \cdot \left. \frac{\Gamma_p\left(\left(-\frac{2}{3} + \frac{j}{p-1}\right)\right) \Gamma_p\left(\left(-\frac{1}{3} + \frac{j}{p-1}\right)\right)}{\Gamma_p\left(\left(-\frac{2}{3}\right)\right) \Gamma_p\left(\left(-\frac{1}{3}\right)\right)} \bar{\omega}^j\left(-\frac{27b^2}{4a^3}\right) \right] \\
 &= \phi(b) \cdot p \cdot {}_2G_2 \left[\begin{matrix} \frac{1}{4}, \frac{3}{4} \\ \frac{1}{3}, \frac{2}{3} \end{matrix} \middle| -\frac{27b^2}{4a^3} \right]_p. \quad \square
 \end{aligned}$$

Remark 4.2. Using (2-7) to evaluate the number of points on certain algebraic varieties over finite fields is by no means new. However, the author first observed the technique in the work of Fuselier [2007; 2010] where it was used to relate these evaluations to hypergeometric functions over finite fields. These methods were subsequently used by Lennon [2011] in generalizing Fuselier's work and, as we've seen, also form part of our proof of Theorem 1.2.

Proof of Corollary 1.3. As noted in the introduction, when $p > 3$, any elliptic curve E/\mathbb{F}_p is isomorphic to an elliptic curve of the form $E' : y^2 = x^3 + ax + b$. Therefore $a_p(E) = a_p(E')$ and Theorem 1.2 can be used to evaluate $a_p(E)$. We also note that

$$j(E) = j(E') = \frac{1728 \cdot 4a^3}{4a^3 + 27b^2},$$

and so

$$1 - \frac{1728}{j(E)} = -\frac{27b^2}{4a^3}.$$

As E and E' are related by an admissible change of variables, this implies $c_6(E) = c_6(E') \cdot u^6$ for some $u \in \mathbb{F}_p^*$. Now $c_6(E') = -27 \cdot 32 \cdot b$ so $\phi(b) = \phi(-6 \cdot c_6(E))$ as required. \square

5. Concluding remarks

5A. The $p = 3$ case. Theorem 1.2 considers elliptic curves over \mathbb{F}_p for primes $p > 3$. While ${}_nG_n[\dots]_p$ is not defined for $p = 2$, it is defined for $p = 3$ once the parameters are 3-adic integers. As the parameters of the ${}_2G_2[\dots]_p$ in Theorem 1.2 are not all 3-adic integers it is clear that the result cannot be extended to $p = 3$ using the same function. However we can say something about the $p = 3$ case. Any elliptic curve over \mathbb{F}_3 , whose j -invariant is nonzero, is isomorphic to a curve

of the form $E : y^2 = x^3 + ax^2 + b$ with both a and b nonzero [Silverman 2009, Appendix A]. It is an easy exercise to evaluate $a_3(E)$ and to show

$$a_3(E) = \phi(a) \cdot {}_2G_2 \left[\begin{matrix} 0, 0 \\ 0, \frac{1}{2} \end{matrix} \middle| -\frac{a}{b} \right]_3.$$

This relationship is somewhat contrived however and direct calculation of $a_3(E)$ is much more straightforward.

5B. Transformation properties of ${}_nG_n[\dots]_p$. As mentioned in Section 3, hypergeometric functions over finite fields were originally defined by Greene [1987] as analogues of classical hypergeometric functions. His motivation was to develop the area of character sums and their evaluations through parallels with the classical functions, and, in particular, with their transformation properties. His endeavor was largely successful and analogues of various classical transformations were found [ibid.]. Some others were recently provided by the author in [McCarthy 2012c]. These transformations for hypergeometric functions over finite fields can obviously be rewritten in terms of ${}_nG_n[\dots]_p$ via Lemma 3.3 and these results will hold for all p where the original characters existed over \mathbb{F}_p . It is an interesting question to consider if these transformations can then be extended to almost all p and become transformations for ${}_nG_n[\dots]_p$ in full generality. This is something yet to be considered and may be the subject of forthcoming work.

5C. q -version of ${}_nG_n[\dots]_p$. As discussed in Section 3, ${}_nG_n[\dots]_p$ extends hypergeometric functions over finite fields, as defined in Definition 3.2, to the p -adic setting. Definition 3.2 can easily be extended to \mathbb{F}_q where q is a prime power and indeed, this is how it was originally defined in [McCarthy 2012c, Definition 1.4]. In a similar manner to the proof of Lemma 3.3, we can then use the Gross–Koblitz formula (not as quoted in Theorem 2.2 but its \mathbb{F}_q -version) to transform the hypergeometric function over \mathbb{F}_q to an expression involving products of the p -adic gamma function. Generalizing the resulting expression yields the following q -version of ${}_nG_n[\dots]_p$. We now let ω denote the Teichmüller character of \mathbb{F}_q .

Definition 5.1. Let $q = p^r$, for p an odd prime and $r \in \mathbb{Z}^+$, and let $t \in \mathbb{F}_q$. For $n \in \mathbb{Z}^+$ and $1 \leq i \leq n$, let $a_i, b_i \in \mathbb{Q} \cap \mathbb{Z}_p$. Then we define

$$\begin{aligned} {}_nG_n \left[\begin{matrix} a_1, a_2, \dots, a_n \\ b_1, b_2, \dots, b_n \end{matrix} \middle| t \right]_q &:= \frac{-1}{q-1} \sum_{j=0}^{q-2} (-1)^{jn} \bar{\omega}^j(t) \\ &\times \prod_{i=1}^n \prod_{k=0}^{r-1} \frac{\Gamma_p \left(\left(a_i - \frac{j}{q-1} \right) p^k \right)}{\Gamma_p \left(\langle a_i p^k \rangle \right)} \frac{\Gamma_p \left(\left(-b_i + \frac{j}{q-1} \right) p^k \right)}{\Gamma_p \left(\langle -b_i p^k \rangle \right)} \\ &(-p)^{- \left[\langle a_i p^k \rangle - \frac{j p^k}{q-1} \right] - \left[\langle -b_i p^k \rangle + \frac{j p^k}{q-1} \right]}. \end{aligned}$$

When $q = p$ in Definition 5.1 we recover ${}_nG_n[\dots]_p$ as per Definition 1.1. We believe ${}_nG_n[\dots]_q$ could be used to generalize results involving hypergeometric functions over \mathbb{F}_q which are restricted to q in certain congruence classes (e.g., those in [Lennon 2011]). However we do not examine this here for the following reason. The main purpose of this paper is to demonstrate that ${}_nG_n[\dots]_p$ can be used to extend results involving hypergeometric functions over \mathbb{F}_p , which are limited to primes in certain congruence classes, and thus avoid the need to work over \mathbb{F}_q .

Acknowledgments

I would like to thank the referee for some helpful comments and suggestions to improve this paper.

References

- [Ahlgren and Ono 2000] S. Ahlgren and K. Ono, “A Gaussian hypergeometric series evaluation and Apéry number congruences”, *J. Reine Angew. Math.* **518** (2000), 187–212. MR 2001c:11057 Zbl 0940.33002
- [Berndt et al. 1998] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons, New York, 1998. MR 99d:11092 Zbl 0906.11001
- [Evans 2010] R. Evans, “Hypergeometric ${}_3F_2(1/4)$ evaluations over finite fields and Hecke eigenforms”, *Proc. Amer. Math. Soc.* **138**:2 (2010), 517–531. MR 2011a:11217 Zbl 05678516
- [Frechette et al. 2004] S. Frechette, K. Ono, and M. Papanikolas, “Gaussian hypergeometric functions and traces of Hecke operators”, *Int. Math. Research Notices* **2004**:60 (2004), 3233–3262. MR 2006a:11055 Zbl 1088.11029
- [Fuselier 2007] J. G. Fuselier, *Hypergeometric functions over finite fields and relations to modular forms and elliptic curves*, Ph.D. thesis, Texas A&M University, 2007, <http://search.proquest.com/docview/304730199>. MR 2710790
- [Fuselier 2010] J. G. Fuselier, “Hypergeometric functions over \mathbb{F}_p and relations to elliptic curves and modular forms”, *Proc. Amer. Math. Soc.* **138**:1 (2010), 109–123. MR 2011c:11068 Zbl 1222.11058
- [Greene 1987] J. Greene, “Hypergeometric functions over finite fields”, *Trans. Amer. Math. Soc.* **301**:1 (1987), 77–101. MR 88e:11122 Zbl 0629.12017
- [Gross and Koblitz 1979] B. H. Gross and N. Koblitz, “Gauss sums and the p -adic Γ -function”, *Ann. of Math. (2)* **109**:3 (1979), 569–581. MR 80g:12015 Zbl 0406.12010
- [Katz 1990] N. M. Katz, *Exponential sums and differential equations*, Annals of Mathematics Studies **124**, Princeton University Press, 1990. MR 93a:14009 Zbl 0731.14008
- [Knapp 1992] A. W. Knap, *Elliptic curves*, Mathematical Notes **40**, Princeton University Press, 1992. MR 93j:11032 Zbl 0804.14013
- [Koblitz 1980] N. Koblitz, *p -adic analysis: a short course on recent work*, London Mathematical Society Lecture Note Series **46**, Cambridge University Press, 1980. MR 82c:12014 Zbl 0439.12011
- [Lennon 2011] C. Lennon, “Gaussian hypergeometric evaluations of traces of Frobenius for elliptic curves”, *Proc. Amer. Math. Soc.* **139**:6 (2011), 1931–1938. MR 2012c:11260 Zbl 05905740
- [McCarthy 2012a] D. McCarthy, “Extending Gaussian hypergeometric series to the p -adic setting”, *Int. J. Number Theory* **8**:7 (2012), 1581–1612. Zbl 06092886

- [McCarthy 2012b] D. McCarthy, “On a supercongruence conjecture of Rodriguez-Villegas”, *Proc. Amer. Math. Soc.* **140**:7 (2012), 2241–2254. MR 2898688
- [McCarthy 2012c] D. McCarthy, “Transformations of well-poised hypergeometric functions over finite fields”, *Finite Fields and Their Applications* **18**:6 (2012), 1133–1147.
- [Mortenson 2005] E. Mortenson, “Supercongruences for truncated ${}_{n+1}F_n$ hypergeometric series with applications to certain weight three newforms”, *Proc. Amer. Math. Soc.* **133**:2 (2005), 321–330. MR 2005f:11080 Zbl 1152.11327
- [Ono 1998] K. Ono, “Values of Gaussian hypergeometric series”, *Trans. Amer. Math. Soc.* **350**:3 (1998), 1205–1223. MR 98e:11141 Zbl 0910.11054
- [Papanikolas 2006] M. Papanikolas, “A formula and a congruence for Ramanujan’s τ -function”, *Proc. Amer. Math. Soc.* **134**:2 (2006), 333–341. MR 2007d:11046 Zbl 1161.11334
- [Silverman 2009] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics **106**, Springer, Dordrecht, 2009. MR 2010i:11005 Zbl 1194.11005
- [Vega 2011] M. V. Vega, “Hypergeometric functions over finite fields and their relations to algebraic curves”, *Int. J. Number Theory* **7**:8 (2011), 2171–2195. MR 2873147 Zbl 06004996

Received May 21, 2012. Revised September 6, 2012.

DERMOT MCCARTHY
DEPARTMENT OF MATHEMATICS
TEXAS A&M UNIVERSITY
MAILSTOP 3368
COLLEGE STATION, TX 77843
UNITED STATES
mccarthy@math.tamu.edu

PACIFIC JOURNAL OF MATHEMATICS

msp.org/pjm

Founded in 1951 by E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

EDITORS

V. S. Varadarajan (Managing Editor)
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
pacific@math.ucla.edu

Paul Balmer
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
balmer@math.ucla.edu

Don Blasius
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
blasius@math.ucla.edu

Vyjayanthi Chari
Department of Mathematics
University of California
Riverside, CA 92521-0135
chari@math.ucr.edu

Daryl Cooper
Department of Mathematics
University of California
Santa Barbara, CA 93106-3080
cooper@math.ucsb.edu

Robert Finn
Department of Mathematics
Stanford University
Stanford, CA 94305-2125
finn@math.stanford.edu

Kefeng Liu
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
liu@math.ucla.edu

Jiang-Hua Lu
Department of Mathematics
The University of Hong Kong
Pokfulam Rd., Hong Kong
jhlu@maths.hku.hk

Sorin Popa
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
popa@math.ucla.edu

Jie Qing
Department of Mathematics
University of California
Santa Cruz, CA 95064
qing@cats.ucsc.edu

Paul Yang
Department of Mathematics
Princeton University
Princeton NJ 08544-1000
yang@math.princeton.edu

PRODUCTION

Silvio Levy, Scientific Editor, production@msp.org

SUPPORTING INSTITUTIONS

ACADEMIA SINICA, TAIPEI
CALIFORNIA INST. OF TECHNOLOGY
INST. DE MATEMÁTICA PURA E APLICADA
KEIO UNIVERSITY
MATH. SCIENCES RESEARCH INSTITUTE
NEW MEXICO STATE UNIV.
OREGON STATE UNIV.

STANFORD UNIVERSITY
UNIV. OF BRITISH COLUMBIA
UNIV. OF CALIFORNIA, BERKELEY
UNIV. OF CALIFORNIA, DAVIS
UNIV. OF CALIFORNIA, LOS ANGELES
UNIV. OF CALIFORNIA, RIVERSIDE
UNIV. OF CALIFORNIA, SAN DIEGO
UNIV. OF CALIF., SANTA BARBARA

UNIV. OF CALIF., SANTA CRUZ
UNIV. OF MONTANA
UNIV. OF OREGON
UNIV. OF SOUTHERN CALIFORNIA
UNIV. OF UTAH
UNIV. OF WASHINGTON
WASHINGTON STATE UNIVERSITY

These supporting institutions contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its contents or policies.


See inside back cover or msp.org/pjm for submission instructions.

The subscription price for 2013 is US \$400/year for the electronic version, and \$485/year for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. The Pacific Journal of Mathematics is indexed by Mathematical Reviews, Zentralblatt MATH, PASCAL CNRS Index, Referativnyi Zhurnal, Current Mathematical Publications and the Science Citation Index.

The Pacific Journal of Mathematics (ISSN 0030-8730) at the University of California, c/o Department of Mathematics, 798 Evans Hall #3840, Berkeley, CA 94720-3840, is published monthly except July and August. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

PJM peer review and production are managed by EditFLOW[®] from Mathematical Sciences Publishers.

PUBLISHED BY

 **mathematical sciences publishers**
nonprofit scientific publishing

<http://msp.org/>

© 2013 Mathematical Sciences Publishers

PACIFIC JOURNAL OF MATHEMATICS

Volume 261 No. 1 January 2013

Hierarchies and compatibility on Courant algebroids	1
PAULO ANTUNES, CAMILLE LAURENT-GENGOUX and JOANA M. NUNES DA COSTA	
A new characterization of complete linear Weingarten hypersurfaces in real space forms	33
CÍCERO P. AQUINO, HENRIQUE F. DE LIMA and MARCO A. L. VELÁSQUEZ	
Calogero–Moser versus Kazhdan–Lusztig cells	45
CÉDRIC BONNAFÉ and RAPHAËL ROUQUIER	
Coarse median spaces and groups	53
BRIAN H. BOWDITCH	
Geometrization of continuous characters of \mathbb{Z}_p^\times	95
CLIFTON CUNNINGHAM and MASOUD KAMGARPOUR	
A note on Lagrangian cobordisms between Legendrian submanifolds of \mathbb{R}^{2n+1}	101
ROMAN GOLOVKO	
On slope genera of knotted tori in 4-space	117
YI LIU, YI NI, HONGBIN SUN and SHICHENG WANG	
Formal groups of elliptic curves with potential good supersingular reduction	145
ÁLVARO LOZANO-ROBLEDO	
Codimension-one foliations calibrated by nondegenerate closed 2-forms	165
DAVID MARTÍNEZ TORRES	
The trace of Frobenius of elliptic curves and the p -adic gamma function	219
DERMOT MCCARTHY	
(DN) - (Ω) -type conditions for Fréchet operator spaces	237
KRZYSZTOF PISZCZEK	



0030-8730(201301)261:1;1-D