JOURNAL OF NUMBER THEORY 52, 125–144 (1995)

On Jacobi Sums, Multinomial Coefficients, and p-adic Hypergeometric Functions

PAUL THOMAS YOUNG

Department of Mathematics, University of Charleston, Charleston, South Carolina 29424

Communicated by Alan C. Woods

Received June 1, 1992; revised June 14, 1993

We extend the methods of our previous article to express certain special values of p-adic hypergeometric functions in terms of the p-adic gamma function and Jacobi sums over general finite fields. These results are obtained via p-adic congruences for Jacobi sums in terms of multinomial coefficients, and allow one to more fully exploit classical hypergeometric identites to obtain p-adic unit root formulae. © 1995 Academic Press, Inc.

1. INTRODUCTION

In [15] we gave some explicit formulae relating Jacobi sums over the prime field $\mathbb{F}_p$ to values of p-adic hypergeometric functions. These formulae were obtained from combinatorial identities and the methods of Dwork ([4, 5]) and Koblitz [7], and may be viewed as p-adic analogues of classical results. The primary focus of this article is the generalization of these results to include Jacobi sums defined over finite extensions of $\mathbb{F}_p$.

We begin in Section 2 by giving congruence results for general Jacobi sums over finite fields of characteristic $p > 2$ in terms of multinomial coefficients. The main tools are the Gross–Koblitz formula and the properties of the p-adic gamma function. For Jacobi sums which are not p-adic units, the congruences we give are stronger than those typically predicted by the theory of formal group laws. We then apply these results to hypergeometric functions in Section 3 to give p-adic analogues of classical formulae. Equation (3.17) below is perhaps the best example (particularly in the case $n = 2m$), and the cohomological interpretation given in [15] remains valid relative to the Frobenius map $(x, y) \mapsto (x^q, y^q)$. The results (3.24), (3.27), (3.28), and (3.44) of [15] may also be extended by the methods found in this paper.

0022-314X/95 $6.00

In Section 4 we consider the elliptic curve with affine equation $y^2 = x^3 - x$ which has supersingular reduction modulo p when $p \equiv -1 \pmod 4$, and show that the roots of its zeta function over $\mathbb{F}_{p^2}$ may be obtained from a limit of p-adic hypergeometric functions, although this is not the specialization of a uniform limit. As a further application, we also express the formal-group congruences associated to an Apéry sequence in terms of Jacobi sums.

2. Jacobi Sums and Multinomial Coefficients

Throughout this paper p will denote an odd prime, $\mathbb{F}_q$ the finite field of $q = p^f$ elements, $\mathbb{Z}_p$ the ring of p-adic integers, $\mathbb{Q}_p$ the field of p-adic numbers, K the unramified extension of $\mathbb{Q}_p$ of degree f, $\mathbb{C}_p$ the completion of an algebraic closure of $\mathbb{Q}_p$, "ord" the valuation on $\mathbb{C}_p$ normalized so that $\operatorname{ord}(p) = 1$, and $\mathfrak{O}$ the ring of integers of $\mathbb{C}_p$. We let $\pi \in \mathfrak{O}$ be a fixed solution to $\pi^{p-1} = -p$ and let ζ be the unique pth root of unity in $\mathfrak{O}$ such that $\zeta \equiv 1 + \pi \pmod{\pi^2 \mathfrak{O}}$.

We define a map $\alpha \mapsto \alpha'$ on $\mathbb{Q} \cap \mathbb{Z}_p$ by requiring that $p\alpha' - \alpha = \mu_\alpha \in \{0, 1, 2, ..., p-1\}$. We write $\alpha^{(0)} = \alpha$, and $\alpha^{(i)} = (\alpha^{(i-1)})'$ for $i > 0$; we also will write $\mu_\alpha^{(i)}$ for $\mu_{\alpha^{(i)}}$. It follows that the $\mu_\alpha^{(i)}$ are the digits in the p-adic expansion of $-\alpha$, that is, $-\alpha = \sum_{i=0}^{\infty} \mu_\alpha^{(i)} p^i$. It is easy to verify that this map is well-defined and continuous; that $\alpha^{(i)} = 0$ for some i if and only if α is zero or a negative integer; and that $\alpha^{(f)} = \alpha$ if and only if α is a rational number in $[0, 1]$ with denominator dividing $q - 1$.

The p-adic gamma function Γ_p is defined for positive integers n by

$$\Gamma_p(n) = (-1)^n \prod_{\substack{0 < j < n \\ p \nmid j}} j, \tag{2.1}$$

and has an extension to a continuous function $\Gamma_p\colon \mathbb{Z}_p \to \mathbb{Z}_p^\times$, which is Lipschitz with constant 1, and satisfies the functional equations of translation and reflection

$$\Gamma_p(x+1) = \begin{cases} -x\Gamma_p(x), & x \in \mathbb{Z}_p^\times, \\ -\Gamma_p(x), & x \in p\mathbb{Z}_p; \end{cases} \tag{2.2}$$

$$\Gamma_p(x)\,\Gamma_p(1-x) = -(-1)^{\mu_x}, \qquad x \in \mathbb{Z}_p. \tag{2.3}$$

Let $\psi\colon \mathbb{F}_p \to \mathbb{Q}_p(\zeta)$ be the additive character on $\mathbb{F}_p$ defined by $\psi(\bar{t}) = \zeta^t$, and let $\psi_f\colon \mathbb{F}_q \to \mathbb{Q}_p(\zeta)$ denote the additive character on $\mathbb{F}_q$ defined by $\psi_f(t) = \psi(\operatorname{Tr}(t))$, where $\operatorname{Tr}\colon \mathbb{F}_q \to \mathbb{F}_p$ is the trace map. The Teichmüller character $\omega_f\colon \mathbb{F}_q \to K$ is the unique multiplicative character on $\mathbb{F}_q$ such that, for all $t \in \mathbb{F}_q$, the reduction of $\omega_f(t)$ mod p is t. (We extend all multiplicative characters χ using the convention $\chi(0)=0$.)

For $\alpha = a/(q-1)$ with $a \in \mathbb{Z}$, the Gauss sum $g(\omega_f^{-a})$ over $\mathbb{F}_q$ associated to the characters ψ_f and ω_f^{-a} is defined by

$$g(\omega_f^{-a}) = -\sum_{t \in \mathbb{F}_q} \psi_f(t)\, \omega_f^{-a}(t). \tag{2.4}$$

Write $a = t(q-1)+c$ with $t, c \in \mathbb{Z}$ and $0 \leqslant c \leqslant q-1$, and put $\gamma = c/(q-1)$; then from the Gross–Koblitz formula [6] we have

$$g(\omega_f^{-a}) = g(\omega_f^{-c}) = \frac{\pi^{S(c)}}{G_1} \cdot \prod_{i=0}^{f-1} \Gamma_p(\gamma^{(i)}), \tag{2.5}$$

where

$$G_1 = \begin{cases} 1, & \text{if } \ c < q-1, \\ q, & \text{if } \ c = q-1, \end{cases} \tag{2.6}$$

and where $S(c)$ denotes the sum of the digits in the base p expansion of c. (Allowing both $c=0$ and $c=q-1$ will be useful later.)

If $s \geqslant 2$ and $\chi_1, ..., \chi_s\colon \mathbb{F}_q \to K$ are multiplicative characters, the Jacobi sum $J(\chi_1, ..., \chi_s)$ is defined by

$$J(\chi_1, ..., \chi_s) = -\sum_{t_1 + \cdots + t_s = 1} \chi_1(t_1) \cdots \chi_s(t_s). \tag{2.7}$$

A modification of ([13, Lemma 6.2]), using the results of [14] or ([9, Theorem 1.1]) shows that

$$J(\chi_1, ..., \chi_s) = \frac{(-1)^s}{G_2} \cdot \frac{g(\chi_1) \cdots g(\chi_s)}{g(\chi_1 \cdots \chi_s)}, \tag{2.8}$$

where

$$G_2 = \begin{cases} 1, & \text{if } \ \chi_1 \cdots \chi_s \text{ is nontrivial}, \\ q, & \text{if } \ \chi_1 \cdots \chi_s \text{ is trivial but each } \chi_j \text{ is nontrivial}. \end{cases} \tag{2.9}$$

The following lemma will be used to relate Jacobi sums to multinomial coefficients via (2.5) and (2.8).

LEMMA 2.1. *Suppose $m_1, ..., m_s$ are nonnegative integers and write $m_j = k_j p + l_j$ with each $l_j \in \{0, 1, ..., p-1\}$; set $m = m_1 + \cdots + m_s$,*

$k = k_1 + \cdots + k_s$, and $l = l_1 + \cdots + l_s$. Let ε be a nonnegative integer and set $\delta = [\![(l+\varepsilon)/p]\!]$. Then

$$\frac{(m+\varepsilon)!\, k_1! \cdots k_s!}{(k+\delta)!\, m_1! \cdots m_s!} = (-p)^{\delta} \frac{\Gamma_p(-m_1) \cdots \Gamma_p(-m_s)}{\Gamma_p(-m-\varepsilon)}.$$

Proof. We note that $(-m_j)' = -k_j$ for each j and $(-m-\varepsilon)' = -k-\delta$. From the definition of Γ_p we have

$$-\Gamma_p(1+m_j) = (-1)^{m_j} p^{-k_j} \frac{m_j!}{k_j!}, \tag{2.10}$$

and a similar expression for $-\Gamma_p(1+m+\varepsilon)$. Therefore we have

$$\frac{(m+\varepsilon)!\, k_1! \cdots k_s!}{(k+\delta)!\, m_1! \cdots m_s!} = (-1)^{s+1+\varepsilon} p^{\delta} \frac{\Gamma_p(1+m+\varepsilon)}{\Gamma_p(1+m_1) \cdots \Gamma_p(1+m_s)}. \tag{2.11}$$

The lemma then follows by applying the reflection formula (2.3), noting that each $\mu_{-m_j} = l_j$ and $\mu_{-m-\varepsilon} = l + \varepsilon - p\delta$.

We now give our principal congruence result for general Jacobi sums.

THEOREM 2.2. *Let $\alpha_1, ..., \alpha_s \in \mathbb{Z}_p \cap \mathbb{Q} \cap [0, 1)$ satisfy $\alpha_j = a_j/(q-1)$ with each $a_j \in \mathbb{Z}$, and set $\alpha = \alpha_1 + \cdots + \alpha_s$. We assume that $\alpha > 0$, and if $\alpha \in \mathbb{Z}$ we also assume each $\alpha_j > 0$. For $r \geqslant 0$ define the nonnegative integers $n_{j,r} = (q^r - 1)\alpha_j$, $n_r = (q^r - 1)\alpha$. Let t be the greatest integer strictly less than α, and suppose $t < p$. Let e be the p-adic ordinal of the Jacobi sum $J(\omega_f^{-a_1}, ..., \omega_f^{-a_s})$. Then for each $r > 0$ we have the congruence*

$$\frac{\dbinom{n_r + t}{n_{1,r}, ..., n_{s,r}, t}}{\dbinom{n_{r-1} + t}{n_{1,r-1}, ..., n_{s,r-1}, t}} \equiv (-1)^s J(\omega_f^{-a_1}, ..., \omega_f^{-a_s}) \pmod{p^{1+e} q^{r-1} \mathbb{Z}_p}.$$

Proof. For $j = 1, ..., s$ we may write $n_{j,r} = \sum_{i=0}^{fr-1} \mu_{\alpha_j}^{(i)} p^i$. For $0 \leqslant i \leqslant f-1$ we will apply Lemma 2.1 with $-m_j = (-n_{j,r})^{(i)}$, so that $-k_j = (-n_{j,r})^{(i+1)}$ and $l_j = \mu_{\alpha_j}^{(i)}$. For each i we choose the nonnegative integer $\varepsilon = \varepsilon_i$ so as to satisfy $(-n_r - t)^{(i)} = -n_{1,r}^{(i)} - \cdots - n_{s,r}^{(i)} - \varepsilon_i$; this implies that $\delta = \varepsilon_{i+1}$ in the notation of the lemma. Thus $\varepsilon_{i+1} = [\![(\mu_{\alpha_1}^{(i)} + \cdots + \mu_{\alpha_s}^{(i)} + \varepsilon_i)/p]\!]$; i.e., ε_{i+1} is the number of carries from the $(i+1)$st to the $(i+2)$nd digit in the base p addition of $a_1 + \cdots + a_s + t$. Writing $\alpha = a/(q-1)$ with $a = (q-1)t + c$ and $0 < c \leqslant q-1$, and setting $\gamma = c/(q-1)$, it follows that $n_r + t = q^r t + (q^r - 1)\gamma$ for each $r \geqslant 0$. From this we see that $(-n_r - t)^{(f)} = -n_{r-1} - t$ for each $r > 0$, implying $\varepsilon_f = \varepsilon_0 = t$.

We take the product on both sides of these equalities from Lemma 2.1, as i runs from 0 to $f-1$. On the left, the product telescopes, yielding

$$\frac{(n_r+t)!\, n_{1,r-1}! \cdots n_{s,r-1}!}{(n_{r-1}+t)!\, n_{1,r}! \cdots n_{s,r}!} = (-p)^e \prod_{i=0}^{f-1} \frac{\Gamma_p((-n_{1,r})^{(i)}) \cdots \Gamma_p((-n_{s,r})^{(i)})}{\Gamma_p((-n_r-t)^{(i)})}, \tag{2.12}$$

where $e = \varepsilon_1 + \cdots + \varepsilon_f$ is the number of carries in the base p addition $a_1 + \cdots + a_s + t$, since we assume $\varepsilon_f = t < p$. Since Γ_p is unit-valued and Lipschitz with constant 1 we have the congruence

$$\prod_{i=0}^{f-1} \frac{\Gamma_p((-n_{1,r})^{(i)}) \cdots \Gamma_p((-n_{s,r})^{(i)})}{\Gamma_p((-n_r-t)^{(i)})} \equiv \prod_{i=0}^{f-1} \frac{\Gamma_p(\alpha_1^{(i)}) \cdots \Gamma_p(\alpha_s^{(i)})}{\Gamma_p(\gamma^{(i)})} \quad (\text{mod } pq^{r-1}\mathbb{Z}_p), \tag{2.13}$$

and therefore

$$\frac{(n_r+t)!\, n_{1,r-1}! \cdots n_{s,r-1}!}{(n_{r-1}+t)!\, n_{1,r}! \cdots n_{s,r}!} \equiv (-p)^e \prod_{i=0}^{f-1} \frac{\Gamma_p(\alpha_1^{(i)}) \cdots \Gamma_p(\alpha_s^{(i)})}{\Gamma_p(\gamma^{(i)})} \quad (\text{mod } p^{1+e}q^{r-1}\mathbb{Z}_p). \tag{2.14}$$

We claim that the right member of the congruence (2.14) is precisely $(-1)^s J(\omega_f^{-a_1}, ..., \omega_f^{-a_s})$. From (2.5) and (2.8), we see that

$$(-1)^s J(\omega_f^{-a_1}, ..., \omega_f^{-a_s}) = \pi^g \cdot \prod_{i=0}^{f-1} \frac{\Gamma_p(\alpha_1^{(i)}) \cdots \Gamma_p(\alpha_s^{(i)})}{\Gamma_p(\gamma^{(i)})}, \tag{2.15}$$

where $g = S(a_1) + \cdots + S(a_s) - S(c)$; note that, since $0 < c \leq q-1$, we have $c = q-1$ if and only if w_f^{-a} is trivial, so that the factors G_1 and G_2 from (2.6) and (2.9) always cancel. Thus we need only show that $e = g/(p-1)$. Since $a + t = tq + c$, we have $S(a+t) = S(tq+c) = S(t) + S(c)$, and therefore $g = S(a_1) + \cdots + S(a_s) + S(t) - S(a+t)$. As it is well-known that $\text{ord}(n!) = (n - S(n))/(p-1)$, we see that $g/(p-1)$ is the ordinal of the multinomial coefficient $\binom{a+t}{a_1, ..., a_s, t}$, which is precisely the number e of carries in the base p addition $a_1 + \cdots + a_s + t$. The proof is now complete.

When $e > 0$ these congruences become stronger than those generally obtained from formal group laws. Considering the simplest case, suppose that $f = 1$ (so $p = q$); then $e = \varepsilon_1 = t$. The result for $s = 2$, $e = 0$ has been given previously ([15, Corollary 2.2]). The congruences of Theorem 2.2 hold modulo $p^{r+t}\mathbb{Z}_p$, and therefore one has the result

$$\binom{n_r+t}{n_{1,r}, ..., n_{s,r}, t} \equiv (-1)^s J(\omega_1^{-a_1}, ..., \omega_1^{-a_s}) \times \binom{n_{r-1}+t}{n_{1,r-1}, ..., n_{s,r-1}, t} \quad (\mathrm{mod}\ p^{(1+t)r}\mathbb{Z}_p), \tag{2.16}$$

since the multinomial coefficient on the right side of (2.16) has p-adic ordinal $(r-1)t$. For $t \geq 1$ such results have been called supercongruences.

A second interesting case is obtained by taking an integer $d > 2$, an odd prime p such that $p \equiv -1 \pmod{d}$, $s = 2$, and $\alpha_1 = \alpha_2 = 1/d$. Taking $f = 2$, $q = p^2$, one then has $e = 1$, $t = 0$, and the congruences read

$$\frac{\binom{2(q^r-1)/d}{(q^r-1)/d}}{\binom{2(q^{r-1}-1)/d}{(q^{r-1}-1)/d}} + p \equiv 0 \quad (\mathrm{mod}\ q^r\mathbb{Z}), \tag{2.17}$$

as it is easily verified from (2.8), (2.5), and (2.3) that $J(\omega_2^{-a_1}, \omega_2^{-a_1}) = -p$. The $r = 1$ case of these congruences has been given in ([8, Proposition 3.1]); in the cases $d = 3$, 4 they arise from formal groups associated to certain supersingular elliptic curves and are related to elliptic cohomology. In Section 4 below we examine the supersingular elliptic curve with $j = 12^3$ which corresponds to the $d = 4$ case.

As the occurrence of the integer t in the multinomial coefficients of Theorem 2.2 is rather artificial, it is natural to remove it, which we now do.

COROLLARY 2.3. *Under the hypotheses of Theorem 2.2, for each $r > 0$ we have the congruence*

$$\frac{\binom{n_r}{n_{1,r}, ..., n_{s,r}}}{\binom{n_{r-1}}{n_{1,r-1}, ..., n_{s,r-1}}} \equiv (-1)^s J(\omega_f^{-a_1}, ..., \omega_f^{-a_s}) \quad (\mathrm{mod}\ p^{b+d+e}q^{r-1}\mathbb{Z}_p),$$

where $d = 0$ if $\mu_\alpha + t < p$ and $d = -1 - \mathrm{ord}(\alpha' - 1)$ if $\mu_\alpha + t \geq p$, and $b = 1 - \mathrm{sgn}(t)$. Furthermore, in all cases we have $b + d + e \geq 1$, so the congruence always holds modulo $pq^{r-1}\mathbb{Z}_p$.

Proof. As before we write $\alpha = a/(q-1)$ with $a = t(q-1)+c$ and $0 < c \leqslant q-1$. If $t=0$ the results are immediate, so assume $1 \leqslant u \leqslant t < p$; then for all $r > 0$ we have

$$\frac{n_{r-1}+u}{n_r+u} = 1 + \frac{(q^{r-1}-q^r)(\alpha/(u-\alpha))}{1+q^r(\alpha/(u-\alpha))}. \tag{2.18}$$

If $\operatorname{ord}(\alpha-u)>0$, then $\mu_\alpha = p-u$, whence $\mu_\alpha + t \geqslant p$; in this case set $-d = \operatorname{ord}(\alpha-u)$, otherwise set $d=0$. In the former case, we note that $\alpha - u = \alpha + \mu_\alpha - p = p(\alpha'-1)$, showing that the two definitions of d coincide. By writing

$$\alpha - u \frac{-qu+(a+u)}{q-1} = \frac{(t-u)q+(c-t+u)}{q-1} \tag{2.19}$$

we see that $-d \leqslant f$, and that $-d = f$ if and only if $c+u=t$, in which case $a+u=tq$ with $t \geqslant 2$ and $\alpha - u = cq/(q-1)$. It follows that the denominator of the right side of (2.18) is a p-adic unit for all $r>0$, and therefore

$$\frac{(n_{r-1}+1)\cdots(n_{r-1}+t)}{(n_r+1)\cdots(n_r+t)} \equiv 1 \qquad (\operatorname{mod} p^d q^{r-1}\mathbb{Z}_p), \tag{2.20}$$

from which it follows that

$$\frac{\begin{pmatrix} n_r \\ n_{1,r}, \ldots, n_{s,r}\end{pmatrix}}{\begin{pmatrix} n_{r-1} \\ n_{1,r-1}, \ldots, n_{s,r-1}\end{pmatrix}} \equiv \frac{\begin{pmatrix} n_r + t \\ n_{1,r}, \ldots, n_{s,r}, t\end{pmatrix}}{\begin{pmatrix} n_{r-1}+t \\ n_{1,r-1}, \ldots, n_{s,r-1}, t\end{pmatrix}} \ (\operatorname{mod} p^{d+e}q^{r-1}\mathbb{Z}_p), \tag{2.21}$$

since the right member of this congruence has p-adic ordinal e. Since $d \leqslant 1$, comparison with Theorem 2.2 proves the first assertion of the corollary.

We now recall that $e = \varepsilon_1 + \cdots + \varepsilon_f$ is the number of carries in the base p addition $a_1 + \cdots + a_s + t$. From (2.19) we see that $\operatorname{ord}(\alpha - u) = \operatorname{ord}(a+u) = -d$. Since the first $-d$ digits of $a+u$ are zero and $a < a+u \leqslant a+t$, we have $\varepsilon_i > 0$ for $0 \leqslant i \leqslant -d$. If $-d < f$ then we have $e \geqslant -d + \varepsilon_f \geqslant -d+1$ since we assume $t = \varepsilon_f \geqslant 1$. If $-d = f$ then $t \geqslant 2$ by the remarks following (2.19); thus all $\varepsilon_i > 0$ and $\varepsilon_f \geqslant 2$, whence $e \geqslant f+1$. Thus $d+e \geqslant 1$ in all cases, completing the proof.

3. Jacobi Sums and p-adic Hypergeometric Functions

We recall from our previous article [15] certain results and definitions concerning the p-adic theory of hypergeometric functions. If $\alpha_1, \ldots, \alpha_k$,

$\gamma_1, \ldots, \gamma_{k-1} \in \mathbb{Q} \cap \mathbb{Z}_p$ and none of the γ_j are zero or negative integers, we denote for $i \geqslant 0$ the hypergeometric series

$$F^{(i)}(X) = {}_kF_{k-1}\left(\begin{matrix}\alpha_1^{(i)}, \ldots, \alpha_k^{(i)} \\ \gamma_1^{(i)}, \ldots, \gamma_{k-1}^{(i)}\end{matrix}; X\right) = \sum_{n=0}^{\infty} A^{(i)}(n)\, X^n$$
$$= \sum_{n=0}^{\infty} \frac{(\alpha_1^{(i)})_n \cdots (\alpha_k^{(i)})_n}{(\gamma_1^{(i)})_n \cdots (\gamma_{k-1}^{(i)})_n\, n!} X^n, \tag{3.1}$$

and for $i, s \geqslant 0$ set $F_s^{(i)}(X) = \sum_{n=0}^{p^s - 1} A^{(i)}(n)\, X^n$. Suppose that the parameters satisfy the conditions

(C1) $|\gamma_j^{(i)}| = 1$ for all $i \geqslant 0$, $j = 1, \ldots, k-1$;

(C2) For each fixed $i \geqslant 0$, supposing the indices are rearranged so that $\mu_{\alpha_1}^{(i)} \leqslant \cdots \leqslant \mu_{\alpha_k}^{(i)}$ and $\mu_{\gamma_1}^{(i)} \leqslant \cdots \leqslant \mu_{\gamma_m}^{(i)}$, where $\gamma_j \neq 1$ for $1 \leqslant j \leqslant m$ and $\gamma_j = 1$ for $m < j \leqslant k-1$, we have $\mu_{\gamma_j}^{(i)} > \mu_{\alpha_{j+1}}^{(i)}$ for $j = 1, \ldots, m$.

Then for all $i \geqslant 0$ we have $F^{(i)}(X) \in \mathbb{Z}_p[\![X]\!]$, and for $r \geqslant s \geqslant 0$ there are formal congruences

$$F_{r+1}^{(i)}(X)\, F_s^{(i+1)}(X^p) \equiv F_r^{(i+1)}(X^p)\, F_{s+1}^{(i)}(X) \qquad (\operatorname{mod} p^{s+1}\mathbb{Z}_p[X]). \tag{3.2}$$

These congruences imply that the ratio $F^{(0)}(x)/F^{(1)}(x^p)$ is the restriction to the disk $\{x \in \mathbb{C}_p : |x| < 1\}$ of the analytic element (i.e., uniform limit of rational functions)

$${}_k\mathfrak{F}_{k-1}\left(\begin{matrix}\alpha_1, \ldots, \alpha_k \\ \gamma_1, \ldots, \gamma_{k-1}\end{matrix}; x\right) = \lim_{r \to \infty} F_{r+1}^{(0)}(x)/F_r^{(1)}(x^p), \tag{3.3}$$

which is supported on the Hasse domain

$$\mathfrak{D} = \{x \in \mathbb{C}_p : |F_1^{(i)}(x)| = 1 \text{ for all } i \geqslant 0\}. \tag{3.4}$$

For series satisfying $F^{(f)} = F^{(0)}$ we will obtain products of Jacobi sums over $\mathbb{F}_q$ as values of the analytic element of support $\mathfrak{D}$ defined by

$${}_k\mathfrak{F}_{k-1}^{(f)}\left(\begin{matrix}\alpha_1, \ldots, \alpha_k \\ \gamma_1, \ldots, \gamma_{k-1}\end{matrix}; x\right) = \lim_{r \to \infty} F_{r+f}^{(0)}(x)/F_r^{(f)}(x^q) \tag{3.5}$$

(cf. [4, p. 42]) whose existence as a uniform limit for $x \in \mathfrak{D}$ follows from the the formal congruences (3.2) and the observation that

$$F_{r+f}^{(0)}(x)/F_r^{(f)}(x^q) = \prod_{i=0}^{f-1} F_{r+f-i}^{(i)}(x^{p^i})/F_{r+f-i-1}^{(i+1)}(x^{p^{i+1}}). \tag{3.6}$$

We note that the limits in (3.3), (3.5) may exist in $\mathbb{Q}_p$ for certain values of $x \in \mathfrak{O}$ not lying in $\mathfrak{D}$, or when the hypotheses (C1), (C2) are not satisfied;

but in this case they need not be specializations of uniform limits. Here we will evaluate the limits (3.3), (3.5) at $x = \pm 1 \in \mathfrak{D}$ for functions satisfying (C1), (C2). Our method will be to p-adically approximate the given series by terminating series which can be evaluated by combinatorial results. For fixed $x_0 \in \mathfrak{D}$ the truncated series $F_s^{(i)}(x_0)$ are rational functions of the parameters $\alpha_j^{(i)}$, $\gamma_j^{(i)}$, and therefore one may appeal to their continuity with respect to the parameters (cf. [7]), although this need not be the case for the nonterminating $F^{(i)}(x_0)$.

We generalize our previous result ([15, Theorem 3.1]) giving a p-adic analogue of Kummer's theorem, which gives the value of a well-poised ${}_2F_1(-1)$.

THEOREM 3.1. *Let T denote the set of all $(\alpha, \beta) \in \mathbb{Z}_p^2$ such that $-1 \in \mathfrak{D}$ and both (C1), (C2) are satisfied for the series $F(X) = {}_2F_1(2\alpha, \beta; 1 + 2\alpha - \beta; X)$. Then $(\alpha, \beta) \in T$ if and only if*

(i) *$2\mu_\alpha^{(i)} \leqslant \mu_\beta^{(i)}$ for all $i \geqslant 0$;*

(ii) *If $\beta \neq 2\alpha$ then $\mu_\beta^{(i)} - \mu_\alpha^{(i)} < (p-1)/2$ for all $i \geqslant 0$.*

Furthermore, if $(\alpha, \beta) \in T$ then

$$ {}_2\mathfrak{F}_1\left(\begin{matrix} 2\alpha, \beta \\ 1 + 2\alpha - \beta \end{matrix}; -1\right) = (-1)^{\mu_\alpha} \frac{\Gamma_p(\alpha)\, \Gamma_p(\beta - \alpha)}{\Gamma_p(2\alpha)\, \Gamma_p(\beta - 2\alpha)}; $$

and if in addition $((q-1)\alpha, (q-1)\beta) = (a, b) \in \{0, 1, ..., q-1\}^2$ then

$$ {}_2\mathfrak{F}_1^{(f)}\left(\begin{matrix} 2\alpha, \beta \\ 1 + 2\alpha - \beta \end{matrix}; -1\right) = (-1)^a \frac{J(\omega_f^{-a}, \omega_f^{a-b})}{J(\omega_f^{-2a}, \omega_f^{2a-b})}. $$

Proof. Suppose $(\alpha, \beta) \in T$, and set $\gamma = 1 + 2\alpha - \beta$. If $\gamma = 1$ then $\beta = 2\alpha$, so $\mu_\beta^{(i)} = \mu_{2\alpha}^{(i)}$ for all i. Since $(\beta - 2\alpha) + \gamma = 1$ we have $\mu_{\beta-2\alpha}^{(i)} + \mu_\gamma^{(i)} = p - 1$ for all i, so if $\gamma \neq 1$ then by (C2) we have $\mu_\gamma^{(i)} > \mu_{2\alpha}^{(i)}, \mu_\beta^{(i)}$, which implies that for all i,

$$ \mu_{2\alpha}^{(i)} + \mu_{\beta-2\alpha}^{(i)} < p - 1, \tag{3.7} $$

$$ \mu_\beta^{(i)} + \mu_{\beta-2\alpha}^{(i)} < p - 1. \tag{3.8} $$

From (3.7) we see that in fact

$$ \mu_{2\alpha}^{(i)} + \mu_{\beta-2\alpha}^{(i)} = \mu_\beta^{(i)} < p - 1, \tag{3.9} $$

so in any event we have $0 \leqslant \mu_{2\alpha}^{(i)} \leqslant \mu_\beta^{(i)}$ for all i.

Since we assume that $F(X)$ satisfies (C1), (C2), we note that

$$ F_1^{(i)}(-1) \equiv {}_2F_1\left(\begin{matrix} -M, -n \\ 1 + n - M \end{matrix}; -1\right) \qquad (\text{mod } p\mathbb{Z}_p), \tag{3.10} $$

where $M=\mu_{2\alpha}^{(i)}$ and $n=\mu_{\beta}^{(i)}$. By equating coefficients of T^M in the expansions of $(1-T)^n(1+T)^n=(1-T^2)^n$ one obtains, for $0\leqslant M\leqslant n$,

$$\sum_{k=0}^{M}(-1)^k\binom{n}{k}\binom{n}{M-k}=\begin{cases}(-1)^m\binom{n}{m}, & \text{if } M=2m,\\ 0, & \text{if } M \text{ is odd.}\end{cases} \tag{3.11}$$

Applying the identity

$$\binom{n}{M-k}=\binom{n}{M}\binom{M}{k}\cdot\binom{n-M+k}{k}^{-1} \tag{3.12}$$

in (3.11) shows that

$$\sum_{k=0}^{M}(-1)^k\frac{\binom{M}{k}\binom{n}{k}}{\binom{n-M+k}{k}}=(-1)^m\frac{\binom{n}{m}}{\binom{n}{2m}} \tag{3.13}$$

if $M=2m\leqslant n$, whereas the sum in (3.13) is zero if M is odd. But since this sum is precisely ${}_2F_1(-M,\ -n;\ 1+n-M;\ -1)$, we see from (3.10) that $-1\notin\mathfrak{D}$ for our $F(X)$ unless $M=\mu_{2\alpha}^{(i)}$ is an even integer for all $i\geqslant 0$.

Since $\mu_{2\alpha}^{(i)}$ must be even for all i, we have $\mu_{2\alpha}^{(i)}=2\mu_{\alpha}^{(i)}$ for all i. From (3.9) we see that $2\mu_{\alpha}^{(i)}\leqslant\mu_{\beta}^{(i)}$ for all i, giving (i). Then substituting the equality in (3.9) into (3.8) yields $2\mu_{\beta}^{(i)}-2\mu_{\alpha}^{(i)}<p-1$, giving (ii).

Now suppose (i) and (ii) hold. From (i) we see that $\mu_{2\alpha}^{(i)}=2\mu_{\alpha}^{(i)}$, $\mu_{\alpha}^{(i)}+\mu_{\beta-\alpha}^{(i)}=\mu_{\beta}^{(i)}$, and $\mu_{2\alpha}^{(i)}+\mu_{\beta-2\alpha}^{(i)}=\mu_{\beta}^{(i)}$ for all i. If $\gamma\neq 1$, then from (ii) we have

$$\begin{aligned}\mu_{\gamma}^{(i)}&=(p-1)-\mu_{\beta-2\alpha}^{(i)}\\&=(p-1)+\mu_{2\alpha}^{(i)}-\mu_{\beta}^{(i)}\\&=(p-1)+2(\mu_{\alpha}^{(i)}-\mu_{\beta}^{(i)})+\mu_{\beta}^{(i)}>\mu_{\beta}^{(i)}\geqslant 2\mu_{\alpha}^{(i)}\geqslant 0,\end{aligned} \tag{3.14}$$

and therefore the hypotheses (C1), (C2) are satisfied for $F(X)$. By comparison with Theorem 2.2, we see that for $m=\mu_{\alpha}^{(i)}$, $n=\mu_{\beta}^{(i)}$, $M=2m$, the binomial coefficients on the right side of (3.13) are p-adic units, showing via (3.10) that $-1\in\mathfrak{D}$. Thus $(\alpha,\beta)\in T$, proving the first statment of the theorem.

The basic idea of Koblitz [7] shows that $(\alpha,\beta)\mapsto{}_2\mathfrak{F}_1(2\alpha,\beta;\ 1+2\alpha-\beta;\ -1)$ is continuous on the set T. For $r>0$ and $(\alpha,\beta)\in T$ set $m_r=\sum_{i=0}^{r-1}\mu_{\alpha}^{(i)}p^i$ and $n_r=\sum_{i=0}^{r-1}\mu_{\beta}^{(i)}p^i$. Since

$$(\mu_{-2m_r}^{(i)},\mu_{-n_r}^{(i)},\mu_{1+n_r-2m_r}^{(i)})=\begin{cases}(\mu_{2\alpha}^{(i)},\mu_{\beta}^{(i)},\mu_{\gamma}^{(i)}), & \text{if } 0\leqslant i\leqslant r,\\ (0,0,1), & \text{if } i\geqslant r,\end{cases} \tag{3.15}$$

we see that $(-2m_r, -n_r) \in T$ as well, because the pair $(0, 0)$ clearly satisfies conditions (i), (ii) above. We note that $(1+2\alpha-\beta)' = 1+2\alpha'-\beta'$ and $(1+n_r-2m_r)' = 1+n'_r-2m'_r$ for all r. Therefore if $s>0$, it follows from (3.2) that there exists $R \geqslant s+1$ such that

$$
\begin{aligned}
{}_2\mathfrak{F}_1\begin{pmatrix}2\alpha, \beta \\ \gamma\end{pmatrix}; -1\Big) &\equiv \frac{F_{s+1}\begin{pmatrix}2\alpha, \beta \\ \gamma\end{pmatrix}; -1\Big)}{F_s\begin{pmatrix}2\alpha', \beta' \\ \gamma'\end{pmatrix}; (-1)^p\Big)} \\
&\equiv \frac{F_{s+1}\begin{pmatrix}-2m_r, -n_r \\ 1+n_r-2m_r\end{pmatrix}; -1\Big)}{F_s\begin{pmatrix}-2m'_r, -n'_r \\ 1+n'_r-2m'_r\end{pmatrix}; (-1)^p\Big)} \\
&\equiv \frac{F\begin{pmatrix}-2m_r, -n_r \\ 1+n_r-2m_r\end{pmatrix}; -1\Big)}{F\begin{pmatrix}-2m'_r, -n'_r \\ 1+n'_r-2m'_r\end{pmatrix}; (-1)^p\Big)} \qquad (\mathrm{mod}\ p^{s+1}\mathbb{Z}_p) \qquad (3.16)
\end{aligned}
$$

for all $r \geqslant R$, the second congruence holding because the $F_s^{(i)}(-1)$ are rational functions of their parameters. We then use (3.13) with $M = 2m_r$, $n = n_r$, and with $M = 2m'_r$, $n = n'_r$, and Lemma 2.1, to obtain

$$
\begin{aligned}
{}_2\mathfrak{F}_1\begin{pmatrix}2\alpha, \beta \\ \gamma\end{pmatrix}; -1\Big) &= \lim_{r\to\infty} \frac{{}_2F_1\begin{pmatrix}-2m_r, -n_r \\ 1+n_r-2m_r\end{pmatrix}; -1\Big)}{{}_2F_1\begin{pmatrix}-2m'_r, -n'_r \\ 1+n'_r-2m'_r\end{pmatrix}; (-1)^p\Big)} \\
&= \lim_{r\to\infty} (-1)^{m_r-m'_r} \frac{\binom{n_r}{m_r}\binom{n'_r}{2m'_r}}{\binom{n'_r}{m'_r}\binom{n_r}{2m_r}} \\
&= \lim_{r\to\infty} (-1)^{m_r-m'_r} \frac{\Gamma_p(-m_r)\,\Gamma_p(m_r-n_r)}{\Gamma_p(-2m_r)\,\Gamma_p(2m_r-n_r)} \\
&= (-1)^{\mu_\alpha} \frac{\Gamma_p(\alpha)\,\Gamma_p(\beta-\alpha)}{\Gamma_p(2\alpha)\,\Gamma_p(\beta-2\alpha)}, \qquad (3.17)
\end{aligned}
$$

as desired.

The Jacobi-sum values of associated ${}_2\mathfrak{F}_1^{(f)}$ for α, β lying also in $(1/(q-1))\,\mathbb{Z} \cap [0, 1]$ may be obtained from (3.17) with the aid of (3.6), (2.5), and (2.8), or directly as follows: Noting that $m_{rf} = (q^r - 1)\,\alpha$, $n_{rf} = (q^r - 1)\,\beta$, $(-2m_{rf})^{(f)} = -2m_{(r-1)f}$, $(-n_{rf})^{(f)} = -n_{(r-1)f}$, and $(1 + n_{rf} - 2m_{rf})^{(f)} = 1 + n_{(r-1)f} - 2m_{(r-1)f}$, we substitute (3.16) in (3.6), yielding

$$
\begin{aligned}
{}_2\mathfrak{F}_1^{(f)}\begin{pmatrix} 2\alpha, \beta \\ \gamma \end{pmatrix}; -1\Bigg) &= \lim_{r \to \infty} \frac{{}_2\mathfrak{F}_1\left(\begin{matrix} -2m_{rf}, -n_{rf} \\ 1 + n_{rf} - 2m_{rf} \end{matrix}; -1\right)}{{}_2F_1\left(\begin{matrix} -2m_{(r-1)f}, -n_{(r-1)f} \\ 1 + n_{(r-1)f} - 2m_{(r-1)f} \end{matrix}; (-1)^q\right)} \\
&= \lim_{r \to \infty} (-1)^{m_{rf} - m_{(r-1)f}} \frac{\binom{n_{rf}}{m_{rf}}\binom{n_{(r-1)f}}{2m_{(r-1)f}}}{\binom{n_{(r-1)f}}{m_{(r-1)f}}\binom{n_{rf}}{2m_{rf}}} \\
&= (-1)^a \frac{J(\omega_f^{-a}, \omega_f^{a-b})}{J(\omega_f^{-2\alpha}, \omega_f^{2a-b})}
\end{aligned}
\tag{3.18}
$$

via (3.13) with $M = 2m_{rf}$, $n = n_{rf}$, and with $M = 2m_{(r-1)f}$, $n = n_{(r-1)f}$, and Corollary 2.3. This completes the proof.

We remark that, by (3.13) and Corollary 2.3, the limit of hypergeometric functions given in (3.18) is indeed correct for any $\alpha, \beta \in (1/(q-1))\,\mathbb{Z} \cap [0, 1]$ such that $2\alpha \leqslant \beta$. However when $(\alpha, \beta) \notin T$ the syumbol ${}_2\mathfrak{F}_1^{(f)}$ is not justified for this limit, as it need not be the specialization to -1 of a uniform limit on that residue class.

We now give a generalization of Dixon's theorem, which gives the value of a well-poised ${}_3\mathfrak{F}_2(1)$. We give a proof along somewhat different lines than the one given in [15] for elements of $(1/((p-1))\,\mathbb{Z}$.

THEOREM 3.2. *Let T denote the set of all $(\alpha, \beta, \gamma) \in \mathbb{Z}_p^3$ such that $1 \in \mathfrak{D}$ and both* (C1), (C2) *are satisfied for the series $F(X) = {}_3F_2(2\alpha, \beta, \gamma; 1 + 2\alpha - \beta, 1 + 2\alpha - \gamma; X)$. Then $(\alpha, \beta, \gamma) \in T$ if and only if*

(i) $2\mu_\alpha^{(i)} \leqslant \mu_\beta^{(i)}, \mu_\gamma^{(i)}$ *and* $\mu_\beta^{(i)} + \mu_\gamma^{(i)} - \mu_\alpha^{(i)} \leqslant p - 1$ *for all* $i \geqslant 0$;

(ii) *If* $2\alpha, \beta, \gamma$ *are not all equal then* $\mu_\beta^{(i)} + \mu_\gamma^{(i)} - 2\mu_\alpha^{(i)} < p - 1$ *for all* $i \geqslant 0$.

Furthermore, if $(\alpha, \beta, \gamma) \in T$ then

$$
\begin{aligned}
&{}_3\mathfrak{F}_2\left(\begin{matrix} 2\alpha, \beta, \gamma \\ 1 + 2\alpha - \beta, 1 + 2\alpha - \gamma \end{matrix}; 1\right) \\
&\quad = (-1)^{\mu_\alpha} \frac{\Gamma_p(\alpha)\,\Gamma_p(\gamma - \alpha)\,\Gamma_p(\beta - \alpha)\,\Gamma_p(\beta + \gamma - 2\alpha)}{\Gamma_p(2\alpha)\,\Gamma_p(\gamma - 2\alpha)\,\Gamma_p(\beta - 2\alpha)\,\Gamma_p(\beta + \gamma - \alpha)};
\end{aligned}
$$

and if in addition $((q-1)\alpha, (q-1)\beta, (q-1)\gamma) = (a, b, c) \in \{0, 1, ..., q-1\}^3$ *then*

$$ {}_3\mathfrak{F}_2^{(f)}\left(\begin{matrix} 2\alpha, \beta, \gamma \\ 1+2\alpha-\beta, 1+2\alpha-\gamma \end{matrix}; 1\right) = (-1)^a \frac{J(\omega_f^{-a}, \omega_f^{2a-b-c})\, J(\omega_f^{-a}, \omega_f^{a-b})}{J(\omega_f^{-a}, \omega_f^{2a-c})\, J(\omega_f^{-2a}, \omega_f^{2a-b})}. $$

Proof. Suppose $(\alpha, \beta, \gamma) \in T$, set $\delta = 1 + 2\alpha - \beta$ and $\varepsilon = 1 + 2\alpha - \gamma$. If $\delta = \varepsilon = 1$ then $2\alpha = \beta = \gamma$, so $\mu_{2\alpha}^{(i)} = \mu_\beta^{(i)} = \mu_\gamma^{(i)}$ for all i. Note that $\mu_{\beta-2\alpha}^{(i)} + \mu_\delta^{(i)} = p-1$ and $\mu_{\gamma-2\alpha}^{(i)} + \mu_\varepsilon^{(i)} = p-1$ for all i. Therefore if δ, ε are not both equal to 1, (C2) implies that for all $i \geqslant 0$, either $\mu_\delta^{(i)} > \mu_{2\alpha}^{(i)}$ or $\mu_\varepsilon^{(i)} > \mu_{2\alpha}^{(i)}$, so that for all i,

$$ \mu_{2\alpha}^{(i)} + \mu_{\beta-2\alpha}^{(i)} < p-1 \qquad \text{or} \qquad \mu_{2\alpha}^{(i)} + \mu_{\gamma-2\alpha}^{(i)} < p-1. \tag{3.19} $$

Now if for some i, say the former half of (3.19) holds, then in fact

$$ \mu_{2\alpha}^{(i)} + \mu_{\beta-2\alpha}^{(i)} \leqslant \mu_\beta^{(i)} \leqslant \mu_{2\alpha}^{(i)} + \mu_{\beta-2\alpha}^{(i)} + 1 \leqslant p-1, \tag{3.20} $$

so in particular $\mu_{2\alpha}^{(i)} \leqslant \mu_\beta^{(i)}$ for such i. But then (C2) requires that both $\mu_\delta^{(i)}, \mu_\varepsilon^{(i)} > \mu_{2\alpha}^{(i)}$, so both inequalities in (3.19) must hold; thus in fact for any i we have

$$ \mu_{2\alpha}^{(i)} + \mu_{\beta-2\alpha}^{(i)} = \mu_\beta^{(i)}, \qquad \mu_{2\alpha}^{(i)} + \mu_{\gamma-2\alpha}^{(i)} = \mu_\gamma^{(i)}, \tag{3.21} $$

so in any event we have $\mu_{2\alpha}^{(i)} \leqslant \mu_\beta^{(i)}, \mu_\gamma^{(i)}$ for all i.

Since we assume that $F(X)$ satisfies (C1), (C2), we note that

$$ F_1^{(i)}(1) \equiv {}_3F_2\left(\begin{matrix} -S, -m, -n \\ 1+m-S, 1+n-S \end{matrix}; 1\right) \qquad (\text{mod } p\mathbb{Z}_p), \tag{3.22} $$

where $S = \mu_{2\alpha}^{(i)}$, $m = \mu_\beta^{(i)}$ and $n = \mu_\gamma^{(i)}$. A terminating from of the classical Dixon's theorem ([10, eq. (III.9)]) states that for $n, m \in \mathbb{Z}^+$, we have

$$ {}_3F_2\left(\begin{matrix} -2s, -m, -n \\ 1+m-2s, 1+n-2s \end{matrix}; 1\right) = \frac{(1-2s)_n\,(1+m-s)_n}{(1-s)_n\,(1+m-2s)_n}(1+m-2s)_n \tag{3.23} $$

if $2s$ is not a positive integer. We invoke the identity $(1+x)_n = \Gamma(1+x+n)/\Gamma(1+x)$ to express each factor on the right side of (3.23) in terms of the classical gamma function. Using the classical functional equations $\Gamma(1+z)=z\Gamma(z)$ and $\Gamma(z)\,\Gamma(1-z)=\pi\csc\pi z$ (here π has its more usual meaning) we obtain

$$\frac{\Gamma(1-s)}{\Gamma(1-2s)}=\frac{\Gamma(1+2s)}{\Gamma(1+s)}\cos\pi s, \tag{3.24}$$

which shows that the value of the ${}_3F_2(1)$ in (3.23) is equal to

$$\cos\pi s\,\frac{\Gamma(1+2s)\,\Gamma(1+n-2s)\,\Gamma(1+m+n-s)\,\Gamma(1+m-2s)}{\Gamma(1+s)\,\Gamma(1+n-s)\,\Gamma(1+m-s)\,\Gamma(1+m+n-2s)}. \tag{3.25}$$

As functions of s, both the ${}_3F_2(1)$ in (3.23) and the expression (3.25) are continuous at s when $2s$ is a positive integer such that $2s\leqslant m, n$, so their equality holds also in this case. Note that if $2s$ is a positive odd integer and $2s\leqslant m, n$ then $\cos\pi s=0$ and the expression (3.25) is therefore zero. Since $\cos\pi N=(-1)^N$ and $\Gamma(1+N)=N!$ for $N\in\mathbb{Z}^+$, we obtain the identity

$${}_3F_2\left(\begin{matrix}-2s,\ -m,\ n\\ 1+m-2s,\ 1+n-2s\end{matrix};1\right)=(-1)^s\frac{\binom{m+n-s}{s}\binom{m}{s}}{\binom{n-s}{s}\binom{m}{2s}}, \tag{3.26}$$

valid for integers positive integers s, n, m such that $2s\leqslant m, n$, whereas this value is zero if $2s$ is a positive odd integer and $2s\leqslant m, n$. Comparing this result with (3.22), we see that $1\notin\mathfrak{D}$ for our $F(X)$ unless $S=\mu_{2\alpha}^{(i)}$ is an even integer for all $i\geqslant 0$. Therefore $\mu_{2\alpha}^{(i)}=2\mu_\alpha^{(i)}$ for all i, giving the first half of (i).

Since $2\mu_\alpha^{(i)}\leqslant\mu_\beta^{(i)}, \mu_\gamma^{(i)}$ for all i, we see that the binomial coefficients $\binom{m}{s}$, $\binom{m}{2s}$, and $\binom{n-s}{s}$ all lie in $\mathbb{Z}_p^\times$, where $s=\mu_\alpha^{(i)}$, $m=\mu_\beta^{(i)}$ and $n=\mu_\gamma^{(i)}$. Comparing (3.22) and (3.26) (with $S=2s$) shows that the ensure $1\in\mathfrak{D}$ we need $\binom{m+n-s}{s}\in\mathbb{Z}_p^\times$ which requires $m+n-s\leqslant p-1$, giving the second half of condition (i).

Finally, if 2α, β, γ are not all equal, then from (C2) we know that for all i, either $\mu_\beta^{(i)}>\mu_\gamma^{(i)}$ or $\mu_\gamma^{(i)}>\mu_\beta^{(i)}$. Thus for all i,

$$\mu_\gamma^{(i)}+\mu_{\beta-2\alpha}^{(i)}<p-1 \qquad\text{or}\qquad \mu_\beta^{(i)}+\mu_{\gamma-2\alpha}^{(i)}<p-1, \tag{3.27}$$

but in either case (3.21) yields $\mu_\beta^{(i)}+\mu_\gamma^{(i)}-2\mu_\alpha^{(i)}<p-1$, which is condition (ii).

Now suppose (i) and (ii) hold. It follows easily that $\mu_{2\alpha}^{(i)}=2\mu_\alpha^{(i)}$ and (3.21) holds for all i. Furthermore, if $2\alpha, \beta, \gamma$ are not all equal, then $\mu_{1+2\alpha-\beta}^{(i)}>\mu_\gamma^{(i)}\geqslant\mu_{2\alpha}^{(i)}$ and $\mu_{1+2\alpha-\gamma}^{(i)}>\mu_\beta^{(i)}\geqslant\mu_{2\alpha}^{(i)}$, so $F(X)$ satisfies (C1) and (C2). From (i) we see that for $s=\mu_\alpha^{(i)}$, $m=\mu_\beta^{(i)}$ and $n=\mu_\gamma^{(i)}$, each binomial coefficient on the right side of (3.26) is a p-adic unit. Then (3.22) shows that $1\in\mathfrak{D}$, proving the first statement of the theorem.

Now let $(\alpha, \beta, \gamma) \in T$, and for $r > 0$ set $s_r = \sum_{i=0}^{r-1} \mu_\alpha^{(i)} p^i$, $m_r = \sum_{i=0}^{r-1} \mu_\beta^{(i)} p^i$, and $n_r = \sum_{i=0}^{r-1} \mu_\gamma^{(i)} p^i$. Since

$$(\mu^{(i)}_{-2s_r}, \mu^{(i)}_{-m_r}, \mu^{(i)}_{-n_r}, \mu^{(i)}_{1+m_r-2s_r}, \mu^{(i)}_{1+n_r-2s_r})$$
$$= \begin{cases} (\mu^{(i)}_{2\alpha}, \mu^{(i)}_{\beta}, \mu^{(i)}_{\gamma}, \mu^{(i)}_{1+2\alpha-\beta}, \mu^{(i)}_{1+2\alpha-\gamma}), & \text{if } 0 \leqslant i < rf, \\ (0, 0, 0, 1, 1), & \text{if } i \leqslant rf, \end{cases} \tag{3.28}$$

we see that $(-2s_r, -m_r, -n_r) \in T$ as well. Therefore, for all $s > 0$ there exists $R \geqslant s+1$ such that

$$
\begin{aligned}
{}_3\mathfrak{F}_2\left(\begin{matrix} 2\alpha, \beta, \gamma \\ 1+2\alpha-\beta, 1+2\alpha-\gamma \end{matrix}; 1\right) &\equiv \frac{F_{s+1}\left(\begin{matrix} 2\alpha, \beta, \gamma \\ 1+2\alpha-\beta, 1+2\alpha-\gamma \end{matrix}; 1\right)}{F_s\left(\begin{matrix} 2\alpha', \beta', \gamma' \\ 1+2\alpha'-\beta', 1+2\alpha'-\gamma' \end{matrix}; 1^p\right)} \\
&\equiv \frac{F_{s+1}\left(\begin{matrix} -2s_r, -m_r, -n_r \\ 1+m_r-2s_r, 1+n_r-2s_r \end{matrix}; 1\right)}{F_s\left(\begin{matrix} -2s'_r, -m'_r, -n'_r \\ 1+m'_r-2s'_r, 1+n'_r-2s'_r \end{matrix}; 1^p\right)} \\
&\equiv \frac{F\left(\begin{matrix} -2s_r, -m_r, -n_r \\ 1+m_r-2s_r, 1+n_r-2s_r \end{matrix}; 1\right)}{F\left(\begin{matrix} -2s'_r, -m'_r, -n'_r \\ 1+m'_r-2s'_r, 1+n'_r-2s'_r \end{matrix}; 1^p\right)} \\
&\qquad (\mathrm{mod}\ p^{s+1}\mathbb{Z}^p)
\end{aligned} \tag{3.29}
$$

for all $r \geqslant R$. Then from (3.26) and Lemma 2.1 we have

$$
\begin{aligned}
{}_3\mathfrak{F}_2\left(\begin{matrix} 2\alpha, \beta, \gamma \\ \delta, \varepsilon \end{matrix}; 1\right) &= \lim_{r\to\infty} \frac{{}_3F_2\left(\begin{matrix} -2s_r, -m_r, -n_r \\ 1+m_r-2s_r, 1+n_r-2s_r \end{matrix}; 1\right)}{{}_3F_2\left(\begin{matrix} -2s'_r, -m'_r, -n'_r \\ 1+m'_r, -2s'_r, 1+n'_r-2s'_r \end{matrix}; 1^p\right)} \\
&= \lim_{r\to\infty} (-1)^{s_r-s'_r} \frac{\binom{m_r+n_r-s_r}{s_r}\binom{m_r}{s_r}\binom{n'_r-s'_r}{s'_r}\binom{m'_r}{2s'_r}}{\binom{m'_r+n'_r-s'_r}{s'_r}\binom{m'_r}{s'_r}\binom{n_r-s_r}{s_r}\binom{m_r}{2s_r}} \\
&= (-1)^{\mu_\alpha} \frac{\Gamma_p(\alpha)\,\Gamma_p(\gamma-\alpha)\,\Gamma_p(\beta-\alpha)\,\Gamma_p(\beta+\gamma-2\alpha)}{\Gamma_p(2\alpha)\,\Gamma_p(\gamma-2\alpha)\,\Gamma_p(\beta-2\alpha)\,\Gamma_p(\beta+\gamma-\alpha)},
\end{aligned} \tag{3.30}
$$

giving the second statement of the theorem.

As in (3.18), the Jacobi-sum values for ${}_3\mathfrak{F}_2^{(f)}(\alpha, \beta, \gamma; \delta, \varepsilon; 1)$ for α, β, γ lying also in $(1/(q-1))\,\mathbb{Z} \cap [0, 1]$ may be obtained by using (3.29), (3.26), (3.6), and Corollary 2.3 to evaluate

$$\lim_{r \to \infty} \frac{{}_3F_2\left(\begin{matrix} -2s_{rf},\ -m_{rf},\ -n_{rf} \\ 1+m_{rf}-2s_{rf},\ 1+n_{rf}-2s_{rf} \end{matrix}; 1\right)}{{}_3F_2\left(\begin{matrix} -2s_{(r-1)f},\ -m_{(r-1)f},\ -n_{(r-1)f} \\ 1+m_{(r-1)f}-2s_{(r-1)f},\ 1+n_{(r-1)f}-2s_{(r-1)f} \end{matrix}; 1^q\right)}$$

$$= \lim_{r \to \infty} (-1)^{s_{rf}-s_{(r-1)f}}$$

$$\times \frac{\binom{m_{rf}+n_{rf}-s_{rf}}{s_{rf}}\binom{m_{rf}}{s_{rf}}\binom{n_{(r-1)f}-s_{(r-1)f}}{s_{(r-1)f}}\binom{m_{(r-1)f}}{2s_{(r-1)f}}}{\binom{m_{(r-1)f}+n_{(r-1)f}-s_{(r-1)f}}{s_{(r-1)f}}\binom{m_{(r-1)f}}{s_{(r-1)f}}\binom{n_{rf}-s_{rf}}{s_{rf}}\binom{m_{rf}}{2s_{rf}}}$$

$$= (-1)^a \frac{J(\omega_f^{-a}, \omega_f^{2a-b-c})\, J(\omega_f^{-a}, \omega_f^{a-b})}{J(\omega_f^{-a}, \omega_f^{2a-c})\, J(\omega_f^{-2a}, \omega_f^{2a-b})}. \tag{3.31}$$

Again, the limit of hypergeometric functions given in (3.31) is correct for any $\alpha, \beta, \gamma \in (1/(q-1))\,\mathbb{Z} \cap [0, 1]$ such that $2\alpha \leqslant \beta, \gamma$, but the symbol ${}_3\mathfrak{F}_2^{(f)}$ is not justified for this limit unless $(\alpha, \beta, \gamma) \in T$.

4. Applications

In ([4, eq. (6.29)]) Dwork showed that for the Legendre family of elliptic curves

$$E_\lambda\colon y^2 = x(x-1)(x-\lambda) \qquad (\lambda \neq 0, 1), \tag{4.1}$$

if $\lambda^q = \lambda$ and the reduction of E_λ to $\mathbb{F}_q$ is non-supersingular then the reciprocal unit root $\alpha(\lambda)$ of the zeta-function of the reduced curve $E_\lambda/\mathbb{F}_q$ is given by

$$\alpha(\lambda) = (-1)^{(q-1)/2}\, {}_2\mathfrak{F}_1^{(f)}\left(\begin{matrix} \frac{1}{2}, \frac{1}{2} \\ 1 \end{matrix}; \lambda\right). \tag{4.2}$$

In [15] we noted that if $p \equiv 1 \pmod 4$ and $q = p$ then $-1 \in \mathfrak{D}$, and the value

$$\alpha(-1) = (-1)^{(p-1)/4}\, J(\omega_1^{(1-p)/4}, \omega_1^{(1-p)/4}) \tag{4.3}$$

follows from (4.2) and our p-adic analogue of Kummer's theorem. However, if $p \equiv -1 \pmod 4$ then the curve E_{-1} has supersingular reduction mod p. Here we show that in this case the roots of the zeta function of E_{-1} over $\mathbb{F}_{p^2}$ are also given by a limit of hypergeometric functions as in (3.18). The symbol ${}_2\mathfrak{F}_1^{(2)}(\frac{1}{2}, \frac{1}{2}; 1; -1)$ is not justified for this limit, however, because it is not the specialization to -1 of a uniform limit on that residue class.

This result is obtained from Corollary 2.3 and a theorem of Stienstra [12] as follows: Taking the double cover $U^2 = T_0 T_1^3 - T_0^3 T_1 = T_0 T_1 (T_0 - T_1)(T_0 + T_1)$ of $\mathbb{P}^1$ as a model of E_{-1} and applying ([12, Theorem 0.1), one obtains the congruences

$$\beta_{mq^r} + a\beta_{mq^{r-1}} + q\beta_{mq^{r-2}} \equiv 0 \qquad (\operatorname{mod} pq^{r-1}\mathbb{Z}), \tag{4.4}$$

where

$$\beta_n = \begin{cases} (-1)^m \binom{2m}{m} = \sum_{k=0}^{2m} \binom{2m}{k}^2 (-1)^k, & \text{if} \quad n = 2m+1, \\ 0, & \text{otherwise}, \end{cases} \tag{4.5}$$

and where $P_1(T) = 1 + aT + qT^2$ is the numerator of the zeta function of E_{-1} over $\mathbb{F}_q$. When $p \equiv -1 \pmod 4$ and $q = p^2$, using the first expression $\beta_{4m+1} = (-1)^m \binom{2m}{m}$ and Corollary 2.3 yields

$$\frac{\beta_{q^r}}{\beta_{q^{r-1}}} \equiv J(\omega_2^{(1-q)/4}, \omega_2^{(1-q)/4}) \qquad (\operatorname{mod} q^r\mathbb{Z}_p), \tag{4.6}$$

since this Jacobi sum has p-adic ordinal $e = 1$. Therefore the ratios $\beta_{q^r}/\beta_{q^{r-1}}$ converge in $\mathbb{Z}_p$, and we also find by induction in (4.6) that $\operatorname{ord} \beta_{q^r} = r$. Setting $m = 1$ and dividing the congruence (4.4) by β_{q^r} then yields

$$1 + a\frac{\beta_{q^{r-1}}}{\beta_{q^r}} + q\frac{\beta_{q^{r-2}}}{\beta_{q^{r-1}}} \cdot \frac{\beta_{q^{r-1}}}{\beta_{q^r}} \equiv 0 \qquad (\operatorname{mod} p^{r-1}\mathbb{Z}_p), \tag{4.7}$$

and then letting $r \to \infty$ in (4.7) shows that the ratios $\beta_{q^{r-1}}/\beta_{q^r}$ in fact converge to a root of $P_1(T)$. We note that in general congruences such as (4.4) do not imply convergence of these ratios in the supersingular case ($\operatorname{ord} a > 0$); in particular when $p \equiv -1 \pmod 4$ and $q = p$ this is evident from (4.5). However, having some other means (such as (4.6)) of establishing convergence, it is then easy to see that the limit is a root of the associated polynomial.

One may also check directly via character sums that the Jacobi sum in (4.6) is in fact the reciprocal root of the zeta function of $y^2 = x^3 - x$ over $\mathbb{F}_{p^2}$; that is, $P(T) = (1 - \alpha T)^2$ with $\alpha = J(\omega_2^{(1-q)/4}, \omega_1^{(1-q)/4})$. Indeed, one easily obtains $J(\omega_2^{(1-q)/4}, \omega_2^{(1-q)/4}) = -p$ as in (2.17); since the reciprocal roots of the zeta function over $\mathbb{F}_p$ are $\pm\sqrt{-p}$, the reciprocal roots over $\mathbb{F}_q$ are both $-p$. Using the second expression $\beta_{4m+1}=\sum_{k=0}^{2m}\binom{2m}{k}^2(-1)^k$ in (4.5) we see that the limit of hypergeometric functions in (3.18) exists when $\alpha=\frac{1}{4}$, $\beta=\frac{1}{2}$, $\gamma=1$, and $f=2$; and (4.6), (4.7) show that the limit is indeed a reciprocal root of the zeta function of E_{-1}, although the root is not a unit root.

One should not expect to obtain the supersingular roots over $\mathbb{F}_p$ is this manner, because they have p-adic ordinal $\frac{1}{2}$ and thus do not lie in $\mathbb{Z}_p$. As noted in ([15, pp. 239, 245]), one may view the Jacobi-sum expression for the limit of hypergeometric functions as arising from the complex multiplication $(x, y)\mapsto(-x, \sqrt{-1}\,y)$ on E_{-1} by the fourth roots of unity; this map commutes with the Frobenius $(x, y)\mapsto(x^q, y^q)$ if and only if $q\equiv 1 \pmod 4$, showing why $f=2$ is necessary to make this argument when $p\equiv -1 \pmod 4$; but in view of ([4, eq. (6.28)]) does not explain why the value is a root of the zeta function, because the limit is not the specialization of a uniform limit.

We conclude with an application to the study of the Apéry numbers. In ([15, Corollary 4.2(iii)]) we proved that

$$\beta_{2,p}=(-1)^{(p-1)/2}\,{}_3\mathfrak{F}_2\left(\begin{matrix}\frac{1}{2}, \frac{1}{2}, \frac{1}{2}\\ 1, 1\end{matrix}; -1\right), \tag{4.8}$$

where $\beta_{2,p}$ is the reciprocal of the p-adic unit root of the polynomial $P_{2,p}(T)=1-(4a^2-2p)\,T+p^2T^2$, whenever $p=a^2+2b^2$ with $a, b\in\mathbb{Z}$; this polynomial is the pth Hecke polynomial associated to a certain cusp from the weight 3 and level 8. The proof was obtained from formal-group congruences associated to the Apéry sequence

$$d(n)=\sum_{k=0}^{n}\binom{n}{k}^3={}_3F_2\left(\begin{matrix}-n, -n, -n\\ 1, 1\end{matrix}; -1\right) \tag{4.9}$$

which were discovered by Stienstra and Beukers [11], and which exhibit $\beta_{2,p}$ as the reciprocal of the p-adic unit root of the zeta function of a certain $K3$-surface. Here we express $\beta_{2,p}$ in terms of Jacobi sums over $\mathbb{F}_p$ and over $\mathbb{F}_{p^2}$ using a classical hypergeometric identity and Theorem 3.1.

The value of the hypergeometric function in (4.8) may be obtained by applying the well-known formula

$${}_3F_2\left(\begin{matrix}2\alpha, \alpha+\beta, 2\beta\\ \alpha+\beta+\frac{1}{2}, 2\alpha+2\beta\end{matrix}; x\right)={}_2F_1\left(\begin{matrix}\alpha, \beta\\ \alpha+\beta+\frac{1}{2}\end{matrix}; x\right)^2 \tag{4.10}$$

of Clausen ([1, p. 185]) with $\alpha=\beta=\frac{1}{4}$. When $p\equiv 1 \pmod 8$ we have $\frac{1}{4}'=\frac{1}{4}$, and so $f=1$ suffices, while if $p\equiv 3 \pmod 8$ we have $\frac{1}{4}'=\frac{3}{4}$ and $\frac{3}{4}'=\frac{1}{4}$, so we take $f=2$ in that case. Since $\frac{1}{2}'=\frac{1}{2}$ in either case, we have

$$
{}_3\mathfrak{F}_2\begin{pmatrix}\frac{1}{2},\frac{1}{2},\frac{1}{2}\\1,1\end{pmatrix};-1\Big)^f={}_3\mathfrak{F}_2^{(f)}\begin{pmatrix}\frac{1}{2},\frac{1}{2},\frac{1}{2}\\1,1\end{pmatrix};-1\Big)
$$

$$
={}_2\mathfrak{F}_1^{(f)}\begin{pmatrix}\frac{1}{4},\frac{1}{4}\\1\end{pmatrix};-1\Big)^2
$$

$$
=J(\omega_f^{(1-q)/8},\omega_f^{(1-q)/8})^2. \tag{4.11}
$$

When $p\equiv 1 \pmod 8$ this yields

$$
\beta_{2,p}=J(\omega_1^{(1-p)/8},\omega_1^{(1-p)/8})^2, \tag{4.12}
$$

while for $p\equiv 3 \pmod 8$ we get

$$
\beta_{2,p}=\varepsilon\cdot J(\omega_2^{(1-p^2)/8},\omega_2^{(1-p^2)/8}) \tag{4.13}
$$

where $\varepsilon=\pm 1$.

The value in (4.12) is readily seen to be consistent with the result of Berndt and Evans ([2, Corollary 3.13]). In like fashion, the value $\varepsilon=-1$ in (4.13) may be determined by comparison with ([3, Theorem 4.6]).

One may also determine a Jacobi sum formula for the p-adic integer $\beta_{3,p}$ appearing in ([15, Corollary 4.2(iv)]) indirectly via (4.10) and the theory of elliptic curves. However, this question appears to remain open for the p-adic integer α_p in ([15, Corollary 4.2(v)]).

References

1. H. Bateman, "Higher Transcendental Functions" (A. Erdélyi, Ed.), Vol. 1, McGraw-Hill, New York, 1953.
2. B. Berndt and R. Evans, Sums of Gauss, Jacobi, and Jacobsthal, *J. Number Theory* **11** (1979), 349–398.
3. B. Berndt and R. Evans, Sums of Gauss, Eisenstein, Jacobi, Jacobsthal and Brewer, *Illinois J. Math.* **23** (1979), 374–437.
4. B. Dwork, p-adic cycles, *Publ. Math. IHES* **37** (1969), 27–115.
5. B. Dwork, On p-adic differential equations IV, *Ann. Sci. École Normale Sup.* **6** (1973), 295–315.
6. B. Gross and N. Koblitz, Gauss sums and the p-adic Γ-function, *Ann. Math.* **109** (1979), 569–581.
7. N. Koblitz, The hypergeometric function with p-adic parameters, *Proc. Queens Number Theory Conf.* (1979), 319–328.
8. P. Landweber, Supersingular elliptic curves and congruences for Legendre polynomials, *in* "Elliptic Curves and Modular Forms in Algebraic Topology," pp. 69–93, Lecture Notes in Math., Vol. 1326, Springer-Verlag, New York, 1988.
9. P. Monsky, "p-adic Analysis and Zeta Functions," Kyoto University Lectures in Mathematics, Kinokuniya, Tokyo, 1970.
10. L. J. Slater, "Generalized Hypergeometric Functions," Cambridge Univ. Press, Cambridge, UK 1966.

11. J. STIENSTRA AND F. BEUKERS, On the Picard–Fuchs equation and the formal Brauer group of certain elliptic $K3$-surfaces, *Math. Ann.* **271** (1985), 269–304.
12. J. STEINSTRA, Formal groups and congruences for L-functions, *Amer. J. Math.* **109** (1987), 1111–1127.
13. L. WASHINGTON, "Introduction to Cyclotomic Fields," Springer-Verlag, New York, 1982.
14. A. WEIL, Numbers of solutions of equations in finite fields, *Bull. Amer. Math. Soc.* **55** (1949), 497–508.
15. P. T. YOUNG, Apéry numbers, Jacobi sums, and special values of generalized p-adic hypergeometric functions, *J. Number Theory* **41** (1992), 231–255.