



ELSEVIER

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt



Supercongruences and complex multiplication



Jonas Kibelbek^{a,*}, Ling Long^b, Kevin Moss^a, Benjamin Sheller^a,
Hao Yuan^a

^a Department of Mathematics, Iowa State University, Ames, IA 50011, USA

^b Louisiana State University, Baton Rouge, LA 70803, USA

ARTICLE INFO

Article history:

Received 16 October 2012

Received in revised form 5 December 2015

Accepted 8 December 2015

Available online 3 February 2016

Communicated by David Goss

MSC:

33C20

11G07

11G15

44A20

Keywords:

Complex multiplication

Truncated hypergeometric series

Supercongruences

Atkin and Swinnerton-Dyer

congruences

ABSTRACT

We study congruences involving truncated hypergeometric series of the form

$${}_3F_2\left(\begin{matrix} 1/2, 1/2, 1/2 \\ 1, 1 \end{matrix}; \lambda\right)_{(mp^s-1)/2} := \sum_{k=0}^{(mp^s-1)/2} ((1/2)_k/k!)^3 \lambda^k$$

where p is a prime and m, s are positive integers. These truncated hypergeometric series are related to the arithmetic of a family of K3 surfaces. For special values of λ , with $s = 1$, our congruences are stronger than those predicted by the theory of formal groups, because of the presence of elliptic curves with complex multiplications. They generalize a conjecture made by Stienstra and Beukers for the $\lambda = 1$ case and confirm some other supercongruence conjectures at special values of λ .

© 2016 Elsevier Inc. All rights reserved.

* Corresponding author.

E-mail addresses: jkibelbek@gmail.com (J. Kibelbek), llong@math.lsu.edu (L. Long), kmoss@iastate.edu (K. Moss), bsheller@iastate.edu (B. Sheller), hyuan@iastate.edu (H. Yuan).

1. Introduction

The hypergeometric series ${}_rF_{r-1}$ is defined as

$${}_rF_{r-1} \left(\begin{matrix} a_1, a_2, \dots, a_r \\ b_1, b_2, \dots, b_{r-1} \end{matrix}; \lambda \right) := \sum_{k=0}^{\infty} \left(\frac{(a_1)_k (a_2)_k \cdots (a_r)_k}{k! (b_1)_k (b_2)_k \cdots (b_{r-1})_k} \right) \lambda^k$$

where $(a)_k := a(a+1) \cdots (a+k-1)$ and where none of the b_i is 0 or a negative integer [5]. The truncated hypergeometric series ${}_rF_{r-1} \left(\begin{matrix} a_1, \dots, a_r \\ b_1, \dots, b_{r-1} \end{matrix}; \lambda \right)_n$ is the degree n polynomial in λ obtained by truncating the hypergeometric series to the sum over k from 0 to n .

In this paper, we study the arithmetic of ${}_3F_2 \left(\begin{matrix} \frac{1}{2}, \frac{1}{2}, \frac{1}{2} \\ 1, 1 \end{matrix}; \lambda \right)_n$; these values are related to a family of K3 surfaces

$$S_\lambda : W^2 = X_1 X_2 X_3 (X_1 - X_2)(X_2 - X_3)(X_3 - \lambda X_1)$$

with generic Picard number 19, that has been studied in [4,17]. The variation of the complex structure of this family is depicted by its Picard–Fuchs differential equation, which is an order-3 ordinary differential equation. Up to multiplication by a scalar, its unique holomorphic solution near 0 is ${}_3F_2 \left(\begin{matrix} \frac{1}{2}, \frac{1}{2}, \frac{1}{2} \\ 1, 1 \end{matrix}; \lambda \right)$. Moreover, the Picard–Fuchs equation of the family S_λ is projectively equivalent to the symmetric square of the Picard–Fuchs equation of

$$E_\lambda : y^2 = (x-1) \left(x^2 - \frac{1}{1-\lambda} \right);$$

see [17]. In terms of arithmetic, if we let $A_p(\lambda) = \#(S_\lambda/\mathbb{F}_p) - p^2 - 1$ and $a_p(\lambda) = p+1 - \#(E_\lambda/\mathbb{F}_p)$, then $A_p(\lambda) = \left(\frac{1-\lambda}{p} \right) (a_p(\lambda)^2 - p)$ [4].¹

Deuring’s argument [10, p. 255] shows that for any $\lambda \in \mathbb{F}_p$,

$$A_p(\lambda) \equiv {}_3F_2(\lambda)_{p-1} \equiv {}_3F_2(\lambda)_{\frac{p-1}{2}} \pmod{p}.$$

More generally Dwork showed in [11] that for any $\lambda \in \mathbb{Z}_p$, there is a p -adic number $\gamma(\lambda)$ such that

$${}_3F_2(\lambda)_{mp^s-1} \equiv \gamma(\lambda) \cdot {}_3F_2(\lambda^p)_{mp^{s-1}-1} \pmod{p^s} \quad (1)$$

for all integers $m, s \geq 1$.

It can be shown that these congruences come from a formal group structure attached to S_λ , as constructed by Stienstra [24]. In particular, when ${}_3F_2(\lambda)_{p-1} \not\equiv 0 \pmod{p}$ (i.e. p ordinary for S_λ), one can use the so-called Shioda–Inose structure of the K3

¹ The surfaces $X_{\tilde{\lambda}}$ with affine model $X_{\tilde{\lambda}} : s^2 = xy(x+1)(y+1)(x+\tilde{\lambda}y)$ studied in [4] are isomorphic to S_λ via $\lambda = -\tilde{\lambda}$, $X_1 = 1$, $X_2 = -1/y$, $X_3 = x/y$, and $W = s/y^3$. Note that our λ is the negative of the $\tilde{\lambda}$ in [4].

surfaces S_λ to show that $\gamma(\lambda) = \left(\frac{1-\lambda}{p}\right) \cdot \alpha_p(\lambda)^2$, with $\alpha_p(\lambda)$ being the unit root of $X^2 - a_p(\lambda)X + p = 0$.

At special values of λ , stronger congruences have been observed for the truncations ${}_3F_2(\lambda)_n$. Such congruences, that are stronger than what can be predicted from the formal group structure, are known as *supercongruences*. For example, Stienstra and Beukers conjectured the following supercongruences involving truncated hypergeometric series in [25], corresponding to our $\lambda = 1$ case: for odd primes p ,

$${}_3F_2\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}; 1\right)_{\frac{p-1}{2}} = \sum_{k=0}^{\frac{p-1}{2}} \left(\frac{(\frac{1}{2})_k}{k!}\right)^3 \equiv b_p \pmod{p^2}$$

where b_p is the p th coefficient of the weight-3 cusp form $\eta(4z)^6$, where $\eta(z) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n)$ with $q = e^{2\pi iz}$, is the eta function. This conjecture was proved by Van Hamme in [29], with subsequent proofs by Ishikawa [14] and Ahlgren [1]. More recently, using a different technique, it is shown in [19] that for any prime $p \equiv 1 \pmod{4}$,

$${}_3F_2\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}; 1\right)_{\frac{p-1}{2}} = -\Gamma_p\left(\frac{1}{4}\right)^4 \pmod{p^3}$$

where $\Gamma_p(\cdot)$ denotes the p -adic Gamma function; there is a similar expression for primes which are congruent to 3 modulo 4.

Similarly, Z.-W. Sun conjectured (see remark 1.4 in [26]) a congruence for the $\lambda = 64$ case:

$${}_3F_2\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}; 64\right)_{\frac{p-1}{2}} = \sum_{k=0}^{\frac{p-1}{2}} \left(\frac{(\frac{1}{2})_k}{k!}\right)^3 (64)^k \equiv a_p \pmod{p^2}$$

where $a_p = 0$ if $p \equiv 3, 5, 6 \pmod{7}$ and $a_p = 4x^2 - 2p$ where $p = x^2 + 7y^2$, $x, y \in \mathbb{Z}$, if $p \equiv 1, 2, 4 \pmod{7}$. In fact, this a_p is just the p th coefficient of $\eta(z)^3\eta(7z)^3$.

We show that such supercongruences occur for ${}_3F_2(\lambda)_n$ whenever the elliptic curve E_λ has complex multiplications (CM):

Theorem 1. *Let λ be an algebraic number such that E_λ has complex multiplications. Let p be a prime and let E_λ have a model defined over \mathbb{Z}_p with good reduction modulo $p\mathbb{Z}_p$. Then*

$${}_3F_2\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}; \lambda\right)_{\frac{p-1}{2}} = \sum_{k=0}^{\frac{p-1}{2}} \left(\frac{(\frac{1}{2})_k}{k!}\right)^3 \lambda^k \equiv \left(\frac{1-\lambda}{p}\right) \alpha_p(\lambda)^2 \pmod{p^2}$$

where $\alpha_p(\lambda) \in \mathbb{Z}_p$ is the unit root of $X^2 - [p+1 - \#(E_\lambda/\mathbb{F}_p)]X + p = 0$ if E_λ is ordinary at p ; and $\alpha_p(\lambda) = 0$ if E_λ is supersingular at p .

This result confirms the conjecture of Sun mentioned above. The rational values of λ such that E_λ has CM are $\lambda = -1, 4, -8, 64, \frac{1}{4}, \frac{-1}{8},$ and $\frac{1}{64}$ [4]; but note that this theorem applies also to algebraic CM values of λ and primes p such that λ can be embedded in \mathbb{Z}_p . For example, E_λ is CM when $\lambda = \frac{7}{8} + \frac{5\sqrt{2}}{8}$, and Theorem 1 applies to both embeddings of λ in \mathbb{Z}_p for $p \equiv \pm 1 \pmod{8}$.

At each CM value λ with $|\lambda| < 1$ in each embedding, there is a Ramanujan-type formula of the form $\sum_{k=0}^{\infty} (ak+1) \left(\frac{(\frac{1}{2})_k}{k!} \right)^3 \lambda^k = \frac{b}{\pi}$ where a, b are algebraic numbers depending on λ . Corresponding supercongruences for $\sum_{k=0}^{\frac{p-1}{2}} (ak+1) \left(\frac{(\frac{1}{2})_k}{k!} \right)^3 \lambda^k$ have been obtained in [8].

We derive the following corollary to Theorem 1 in section 4:

Corollary 2. *Let H_k be the harmonic sum $\sum_{j=1}^k \frac{1}{j}$. If E_λ is a CM elliptic curve, then for almost all primes p such that λ embeds in \mathbb{Z}_p ,*

$$\sum_{i=0}^{\frac{p-1}{2}} \binom{2i}{i}^3 \left(\frac{\lambda}{64} \right)^i \left(6(H_{2i} - H_i) + \left(\frac{(\frac{\lambda}{64})^{p-1} - 1}{p} \right) \right) \equiv 0 \pmod{p}.$$

Below is one simple, special case of these congruences for $\lambda = 64$.

Corollary 3. *For all primes $p > 3$, we have*

$$\sum_{i=1}^{\frac{p-1}{2}} \binom{2i}{i}^3 \sum_{j=1}^i \frac{1}{i+j} \equiv 0 \pmod{p}. \quad (2)$$

In general, such congruences are difficult to prove. For similar work, see [1,3] and Remark 1 of [18].

Here are some other well-known examples of supercongruences. Beukers conjectured that for all odd primes p

$${}_4F_3 \left(\frac{1-p}{2}, \frac{1-p}{2}, \frac{1+p}{2}, \frac{1+p}{2}; 1 \right) \equiv c_p \pmod{p^2}$$

where the left hand side² is the $\frac{p-1}{2}$ th Apéry number $\sum_{k=0}^{(p-1)/2} \binom{(p-1)/2}{k}^2 \binom{(p-1)/2+k}{k}^2$ and c_p is the p th coefficient of the weight-4 modular form $\eta(2z)^4 \eta(4z)^4$.

In [22], Rodriguez-Villegas made many supercongruence conjectures, including that for all odd primes p

² Note that this hypergeometric series terminates after the $\frac{p-1}{2}$ th term, because of the negative integer argument $\frac{1-p}{2}$, while Rodriguez-Villegas's conjecture that follows is a genuine truncation.

$${}_4F_3\left(\begin{matrix} \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2} \\ 1, 1, 1 \end{matrix}; 1\right)_{(p-1)/2} \equiv c_p \pmod{p^3}.$$

Ahlgren and Ono proved the modulo p^2 conjecture of Beukers using Gaussian hypergeometric functions (see [3] and [21, Chapter 11]). Kilbourn applied these methods to prove the modulo p^3 conjecture of Rodriguez-Villegas [15], and McCarthy proved another of Rodriguez-Villegas's modulo p^3 conjectures using a p -adic analogue of Gaussian hypergeometric functions [20].

We end our introduction with another motivation for supercongruences. It is known that the coefficients of weight- k noncongruence modular forms satisfy the so-called Atkin and Swinnerton-Dyer congruences [6,23]. These congruences are supercongruences if $k > 2$ [23] and have played an important role in understanding the characterizations of genuine noncongruence modular forms [16].

The paper is organized as follows. We present some background in Section 2. Section 3 discusses supercongruences and uses a theorem of Coster and van Hamme to show that the function ${}_3F_2(\lambda)_n$ exhibits supercongruences whenever E_λ has CM. In section 4, we relate these supercongruences to some interesting combinatorial congruences.

2. Preliminaries

2.1. Legendre polynomials

Let $P_n(x)$ denote the n th Legendre polynomial, which can be defined by $P_n(x) = \frac{1}{2^n n!} \frac{d^n}{dx^n} (x^2 - 1)^n$ [5,9,28]. Equivalently, the degree n Legendre polynomial can be defined as

$$P_n(x) := {}_2F_1\left(-n, n+1; \frac{1-x}{2}\right) = \sum_{k=0}^n \binom{n}{k} \binom{-n-1}{k} \left(\frac{1-x}{2}\right)^k. \quad (3)$$

The first few Legendre polynomials are $P_0(x) = 1$, $P_1(x) = x$, and $P_2(x) = \frac{1}{2}(3x^2 - 1)$. These polynomials form an important class of orthogonal polynomials and have several nice properties; one relevant to our application is that they have generating function $(1 - 2xt + t^2)^{-1/2} = \sum_{n=0}^{\infty} P_n(x)t^n$. Because of this, special values of $P_n(x)$ show up in certain expansions of differential forms on elliptic curves.

2.2. The Atkin and Swinnerton-Dyer congruences

For elliptic curves of the form $\mathcal{E} : y^2 = x(x^2 + Ax + B)$ defined over \mathbb{Z}_p with $t = x/y$ as a local parameter at the point at infinity (where t has a simple zero), Coster and van Hamme showed that the coefficients of the t -expansion of the invariant differential form $-\frac{dx}{2y}$ of \mathcal{E} come from special values of Legendre polynomials (see formula (1) of [9]). Explicitly,

$$-\frac{dx}{2y} = \sum_{k=0}^{\infty} a_k t^k \frac{dt}{t} = \sum_{k=0}^{\infty} P_k \left(\frac{A}{\sqrt{A^2-4B}} \right) (\sqrt{A^2-4B})^k t^{2k+1} \frac{dt}{t}, \quad (4)$$

where $a_{2k+1} = P_k \left(\frac{A}{\sqrt{A^2-4B}} \right) (\sqrt{A^2-4B})^k$ and $a_{2k} = 0$.

The Atkin and Swinnerton-Dyer congruences (ASD) for elliptic curves (Theorem 4 of [6]) imply that if \mathcal{E} has good reduction modulo p , then for all positive integers m and for $s \geq 0$,

$$a_{mp^{s+1}} - A_p a_{mp^s} + p a_{mp^{s-1}} \equiv 0 \pmod{p^{s+1}} \quad (5)$$

where $A_p = p + 1 - \#(\mathcal{E}/\mathbb{F}_p)$. We define a_k to be 0 if k is not integral, as may happen for the final term if $s = 0$.

Essentially, the ASD congruences say that for fixed p and m , terms of the sequence $\{a_{mp^s}\}$ satisfy a three-term congruence with increasing p -adic precision as s increases. The ASD congruences generalize the Hecke recursion: Fourier coefficients b_n of weight $k = 2$, normalized Hecke newforms with trivial nebentypus satisfy the three-term recursion, for all positive integers m , for $s \geq 0$, and for all p ,

$$b_{mp^{s+1}} - b_p b_{mp^s} + p b_{mp^{s-1}} = 0. \quad (6)$$

In the ASD congruences for an elliptic curve \mathcal{E} , we distinguish two cases. If the middle coefficient A_p is divisible by p , we say that \mathcal{E} is *supersingular* at p or simply that p is supersingular. Otherwise, we say \mathcal{E} is *ordinary* at p or that p is ordinary. Dwork's congruences, in which consecutive ratios of certain terms in a sequence converge to a p -adic limit, are related to ASD congruences at ordinary primes. If p is ordinary and is unramified in $K_p := \mathbb{Q}_p(\sqrt{A^2-4B})$, let β_p be the p -adic unit root of $T^2 - [p+1 - \#(\mathcal{E}/\mathbb{F}_p)]T + p$. Then the ASD congruences imply that $a_{mp^s} \equiv \beta_p \cdot a_{mp^{s-1}} \pmod{p^s}$. Using the relation between a_{2k+1} and the Legendre polynomial, we have for any good odd ordinary prime p for \mathcal{E} unramified at K_p

$$P_{\frac{mp^{s-1}}{2}} \left(\frac{A}{\sqrt{A^2-4B}} \right) \equiv \chi_p^{mp^{s-1}} \cdot \beta_p \cdot P_{\frac{mp^{s-1}-1}{2}} \left(\frac{A}{\sqrt{A^2-4B}} \right) \pmod{p^s}, \quad (7)$$

where $\chi_p \in K_p$ is the (not necessarily primitive) order-4 root of unity satisfying $\chi_p \equiv \left(\frac{1}{\sqrt{A^2-4B}} \right)^{\frac{p-1}{2}} \pmod{p}$.

2.3. Clausen formula

It follows from the well-known Clausen formula for hypergeometric series and a Pfaff transformation that

$${}_2F_1 \left(-a, \frac{a+1}{1}; \frac{1 \pm \sqrt{1-x}}{2} \right)^2 = {}_3F_2 \left(\frac{1}{2}, -a, \frac{a+1}{1}; \frac{1}{1}, \frac{1}{1}; x \right). \quad (8)$$

See equation (3.3) of [8] for a derivation of this formula.

Thus,

$$P_n(\sqrt{1-\lambda})^2 = {}_3F_2\left(\begin{matrix} \frac{1}{2}, -n, n+1 \\ 1, 1 \end{matrix}; \lambda\right). \quad (9)$$

The following congruence of degree $(p-1)/2$ polynomials holds coefficient-wise.

Lemma 4. *Let p be any odd prime. Then*

$${}_3F_2\left(\begin{matrix} \frac{1}{2}, \frac{1-p}{2}, \frac{1+p}{2} \\ 1, 1 \end{matrix}; x\right) \equiv {}_3F_2\left(\begin{matrix} \frac{1}{2}, \frac{1}{2}, \frac{1}{2} \\ 1, 1 \end{matrix}; x\right) \pmod{p^2\mathbb{Z}_p[x]}.$$

Proof. We use Zudilin's observation about rising factorials (see Lemma 1 in [7], [18]),

$$\begin{aligned} \left(\frac{1}{2} + \epsilon\right)_k &= \left(\frac{1}{2} + \epsilon\right) \left(\frac{1}{2} + \epsilon + 1\right) \cdots \left(\frac{1}{2} + \epsilon + k - 1\right) \\ &= \left(\frac{1}{2}\right)_k \left(1 + 2\epsilon \sum_{j=1}^k \frac{1}{2j-1} + O(\epsilon^2)\right), \end{aligned}$$

to expand $(\frac{1+p}{2})_k$ in terms of $(\frac{1}{2})_k$. When we take the product $(\frac{1-p}{2})_k (\frac{1+p}{2})_k$, the coefficients of p^1 cancel; and so the product is congruent to $(\frac{1}{2})_k^2$ modulo p^2 , which establishes the coefficient-wise congruence. \square

3. Supercongruences

To prove our main theorem, we use the following theorem of Coster and van Hamme.

Theorem 5 (Coster and van Hamme, [9]). *Let p be an odd prime. Let d be a square-free positive integer such that $(\frac{-d}{p}) = 1$. Let K be an algebraic number field such that $\sqrt{-d} \in K$ and $K \subset \mathbb{Q}_p$. Consider the elliptic curve*

$$\mathcal{E} : Y^2 = X(X^2 + AX + B)$$

with $A, B \in K$, where A and $\Delta = A^2 - 4B$ are p -adic units. Let ω and ω' be a basis of periods of \mathcal{E} and suppose that $\tau = \omega'/\omega \in \mathbb{Q}(\sqrt{-d})$ (which implies that the curve has complex multiplication), τ has positive imaginary part, and $A = 3\wp(\frac{1}{2}\omega)$, $\sqrt{\Delta} = \wp(\frac{1}{2}\omega' + \frac{1}{2}\omega) - \wp(\frac{1}{2}\omega')$, where \wp is the Weierstrass \wp -function. Let $\pi, \bar{\pi} \in \mathbb{Q}(\sqrt{-d})$ such that $\pi\bar{\pi} = p$, with $\bar{\pi}$ a p -adic unit, $\pi = u_1 + v_1\tau$, and $\pi\tau = u_2 + v_2\tau$ with u_1, v_1, u_2, v_2 integers and v_1 even. Then we have

$$P_{\frac{mp^{r-1}}{2}}\left(\frac{A}{\sqrt{\Delta}}\right) \equiv \varepsilon^{mp^{r-1}} \cdot \bar{\pi} \cdot P_{\frac{mp^{r-1}-1}{2}}\left(\frac{A}{\sqrt{\Delta}}\right) \pmod{\pi^{2r}}, \quad (10)$$

where m and r are positive integers, with m odd, and $\varepsilon = (\sqrt{-1})^{-u_2 v_2 + v_2 + p - 2}$, where $P_n(x)$ is the n th Legendre polynomial.

The main point of the theorem is the existence of supercongruences arising from an elliptic curve \mathcal{E} with complex multiplication. While Coster and van Hamme interpreted the congruence as inclusion in an ideal of the ring of integers of K , we interpret all of our congruences p -adically. Since the number field K embeds into \mathbb{Q}_p and π is just p times a p -adic unit under this embedding, we may simply replace $(\bmod \pi^{2r})$ with $(\bmod p^{2r})$ when we view the congruence p -adically. These congruences are twice as strong as formal group theory predicts.

Note that ε and $\bar{\pi}$ in the theorem above must correspond to $\pm\chi_p$ and $\pm\beta_p$ (with the same sign) in our notation. The conditions that τ has positive imaginary part, that $A = 3\wp(\frac{1}{2}\omega)$, and that $\sqrt{\Delta} = \wp(\frac{1}{2}\omega' + \frac{1}{2}\omega) - \wp(\frac{1}{2}\omega')$, can always be satisfied by a suitable choice of the basis of periods; and we can additionally ensure that $\varepsilon = \chi_p$ and $\bar{\pi} = \beta_p$.

Proposition 6. For CM values λ of the family $E_\lambda : y^2 = (x-1)(x^2 - \frac{1}{1-\lambda})$, such that $\lambda \in \mathbb{Z}_p$ and p is ordinary, for all positive integers m and s with m odd,

$${}_3F_2\left(\frac{1}{2}, \frac{1-mp^s}{2}, \frac{1+mp^s}{2}; \lambda\right) \equiv \left(\frac{1-\lambda}{p}\right) \cdot \alpha_p(\lambda)^2 \cdot {}_3F_2\left(\frac{1}{2}, \frac{1-mp^{s-1}}{2}, \frac{1+mp^{s-1}}{2}; \lambda\right) \pmod{p^{2s}}$$

where $\alpha_p(\lambda)$ is the unit root of $X^2 - [p+1 - \#(E_\lambda/\mathbb{F}_p)]X + p = 0$.

Proof. Letting $X = x-1$, $Y = y$, the elliptic curve E_λ can be rewritten as $Y^2 = X(X^2 + 2X + \frac{\lambda}{\lambda-1})$. Then we have $A = 2$, $B = \frac{\lambda}{\lambda-1}$, $\Delta = A^2 - 4B = \frac{4}{1-\lambda}$, and $\frac{A}{\sqrt{A^2-4B}} = \sqrt{1-\lambda}$.

By our assumptions that E_λ has complex multiplication, that $\lambda \in \mathbb{Z}_p$, and that p is ordinary, we satisfy the conditions of Theorem 5: $K = \mathbb{Q}(\lambda)$ embeds into \mathbb{Q}_p and $\lambda \not\equiv 1 \pmod{p}$, so Δ is a p -adic unit. Combining (9) and (10), we have

$$\begin{aligned} {}_3F_2\left(\frac{1}{2}, \frac{1-mp^s}{2}, \frac{1+mp^s}{2}; \lambda\right) &= P_{\frac{mp^s-1}{2}}(\sqrt{1-\lambda})^2 \\ &\equiv (\varepsilon^{mp^{s-1}} \bar{\pi})^2 \cdot P_{\frac{mp^{s-1}-1}{2}}(\sqrt{1-\lambda})^2 \pmod{p^{2s}} \\ &= (\chi_p^{mp^{s-1}} \beta_p)^2 \cdot {}_3F_2\left(\frac{1}{2}, \frac{1-mp^{s-1}}{2}, \frac{1+mp^{s-1}}{2}; \lambda\right) \\ &= \left(\frac{1-\lambda}{p}\right) \cdot \alpha_p(\lambda)^2 \cdot {}_3F_2\left(\frac{1}{2}, \frac{1-mp^{s-1}}{2}, \frac{1+mp^{s-1}}{2}; \lambda\right). \end{aligned}$$

For the final equality, note that we have chosen A and B so that $\beta_p = \alpha_p(\lambda)$ and so that χ_p^2 is the Legendre symbol $\left(\frac{1-\lambda}{p}\right)$, which does not change when we raise it to the odd power mp^{s-1} . \square

Proof of Theorem 1. Note that for all primes p that are ordinary for E_λ , Theorem 1 follows from Proposition 6 and Lemma 4. For primes p that are supersingular for E_λ ,

we can conclude from the ASD congruence that $P_{\frac{p-1}{2}}(\sqrt{1-\lambda}) \equiv 0 \pmod{p}$. Hence ${}_3F_2\left(\frac{\frac{1}{2}, \frac{1}{2}, \frac{1}{2}}{1, 1}; \lambda\right)_{\frac{p-1}{2}} \equiv {}_3F_2\left(\frac{\frac{1}{2}, \frac{1-p}{2}, \frac{1+p}{2}}{1, 1}; \lambda\right) = P_{\frac{p-1}{2}}(\sqrt{1-\lambda})^2 \equiv 0 \pmod{p^2}$, which concludes the proof. \square

We note that this establishes, modulo p^2 , all cases of Conjecture 5.2 of [26] by Z.-W. Sun. These conjectures can be written as

$$\sum_{k=0}^{\frac{p-1}{2}} \binom{2k}{k}^3 \left(\frac{\lambda}{64}\right)^k \equiv \begin{cases} \left(\frac{c}{p}\right) (4a^2 - 2p) \pmod{p^2} & \text{if } \left(\frac{p}{D}\right) = 1 \text{ where } a^2 + Db^2 = p \\ 0 \pmod{p^2} & \text{if } \left(\frac{p}{D}\right) = -1 \end{cases},$$

with appropriate choices of $D \in \mathbb{Z}_+$ and character $\left(\frac{c}{p}\right)$. Note that $\sum_{k=0}^{\frac{p-1}{2}} \binom{2k}{k}^3 \left(\frac{\lambda}{64}\right)^k = {}_3F_2\left(\frac{\frac{1}{2}, \frac{1}{2}, \frac{1}{2}}{1, 1}; \lambda\right)_{\frac{p-1}{2}}$ via the identity $\frac{(1/2)_k^3}{k!^3} = \binom{2k}{k}^3 \frac{1}{64^k}$. These conjectures address the λ -values $\lambda = -8, 1, -\frac{1}{8}, 4, \frac{1}{4}, 64, \frac{1}{64}, -1$, which are all of the CM values for E_λ over \mathbb{Q} , as verified in [4], with the exception of the degenerate case $\lambda = 1$, for which E_λ is not an elliptic curve. The supercongruence for $\lambda = 1$ was proved by Van Hamme in [30] and by Ono in [21].

If E_λ has CM over $K = \mathbb{Q}(\sqrt{-D})$, then the attached 2-dimensional representation ρ decomposes into 2 Grossencharacters when ρ is restricted to $\text{Gal}(\overline{\mathbb{Q}}/K)$. At splitting primes p , which are precisely the ordinary primes of E_λ , the trace of the Frobenius is $\alpha_p(\lambda) + \beta_p(\lambda)$, where both $\alpha_p(\lambda)$ and $\beta_p(\lambda)$ are in the ring of integers of the quadratic field K and have absolute value \sqrt{p} . In the case that K has class number 1 (all Sun λ values correspond to class number 1 cases), then ideals $(\alpha_p(\lambda))$ and $(\beta_p(\lambda))$ are the two distinct prime ideals above p . That is, $\alpha_p(\lambda) = a + b\sqrt{-D}$ and $\beta_p(\lambda) = a - b\sqrt{-D} = \frac{p}{\alpha_p(\lambda)}$, where a and b are integers or half integers depending on $D \equiv 1$ or $3 \pmod{4}$, such that $a^2 + b^2D = p$. In the ordinary case, our congruences involve $\alpha_p(\lambda)^2$, which is just $a^2 - Db^2 + 2ab\sqrt{-D}$. Using $\beta_p(\lambda)^2 = a^2 - Db^2 - 2ab\sqrt{-D} \equiv 0 \pmod{p^2}$ and $a^2 + b^2D = p$, we have $\alpha_p(\lambda)^2 \equiv 4a^2 - 2p \pmod{p^2}$, which, along with the character $\left(\frac{1-\lambda}{p}\right)$, is the target of Z.-W. Sun's congruences in the case that $\left(\frac{p}{D}\right) = 1$. In the case that $\left(\frac{p}{D}\right) = -1$, p is a supersingular prime of E_λ and so ${}_3F_2\left(\frac{\frac{1}{2}, \frac{1}{2}, \frac{1}{2}}{1, 1}; \lambda\right)_{\frac{p-1}{2}} \equiv 0 \pmod{p^2}$, establishing the other half of Z.-W. Sun's congruences.

Alternatively, we note that Ono has explicitly identified the values $\alpha_p(\lambda)$, for all CM curves E_λ with $\lambda \in \mathbb{Z}$, in Theorem 6 of [21]. These values $\alpha_p(\lambda)$ determine the formal group structure and the ASD congruences (i.e., that $\alpha_p(\lambda) \equiv \left(\frac{1-\lambda}{p}\right) \alpha_p(\lambda)^2 \pmod{p}$); combining this with Coster and Van Hamme's supercongruences gives another proof of Sun's conjectures, that $\alpha_p(\lambda) \equiv \left(\frac{1-\lambda}{p}\right) \alpha_p(\lambda)^2 \pmod{p^2}$.

Theorem 1, and the following **Conjecture 7**, apply not only to the cases considered by Ono and Z.-W. Sun, which correspond to CM values of λ over \mathbb{Q} , but also to infinitely many other algebraic CM values of λ , for those primes p such that λ embeds in \mathbb{Z}_p with

$\lambda \not\equiv 0, 1 \pmod{p}$. This is satisfied by almost all primes p such that there is a prime ideal \mathfrak{p} above p in $\mathbb{Q}(\lambda)$ with inertia degree 1.

Based on numeric evidence, we have

Conjecture 7. For CM values λ of the family $E_\lambda : y^2 = (x-1)(x^2 - \frac{1}{1-\lambda})$, such that $\lambda \in \mathbb{Z}_p$ and p is ordinary, for all positive integers m and s with m odd,

$${}_3F_2\left(\begin{matrix} \frac{1}{2}, \frac{1}{2}, \frac{1}{2} \\ 1, 1 \end{matrix}; \lambda\right)_{\frac{mp^s-1}{2}} \equiv \left(\left(\frac{1-\lambda}{p}\right) \alpha_p(\lambda)^2\right) {}_3F_2\left(\begin{matrix} \frac{1}{2}, \frac{1}{2}, \frac{1}{2} \\ 1, 1 \end{matrix}; \lambda\right)_{\frac{mp^{s-1}-1}{2}} \pmod{p^{3s}}$$

where $\alpha_p(\lambda)$ is the unit root of $X^2 - [p+1 - \#(E_\lambda/\mathbb{F}_p)]X + p = 0$.

4. Corollaries

An idea of Gessel for dealing with the supercongruences of the Apéry numbers

$$c_n = {}_4F_3\left(\begin{matrix} -n, -n, 1+n, 1+n \\ 1, 1, 1 \end{matrix}; 1\right) = \sum_{k=0}^n \binom{n}{k}^2 \binom{n+k}{k}^2$$

is as follows [12]. He identified the auxiliary sequence $d_n = 2 \sum_{k=0}^n \binom{n}{k}^2 \binom{n+k}{k}^2 (H_{n+k} - H_{n-k})$, where H_k is the harmonic sum $\sum_{j=1}^k \frac{1}{j}$, and showed that $c_{k+pn} \equiv (c_k + pnd_k)c_n \pmod{p^2}$ where $0 \leq k < p$. Using the idea of Ishikawa [13], we take $k = n = \frac{p-1}{2}$. It follows that when $c_{(p-1)/2} \not\equiv 0 \pmod{p}$, we have the supercongruence $c_{(p^2-1)/2} \equiv c_{(p-1)/2}^2 \pmod{p^2}$ precisely when $d_{(p-1)/2} \equiv 0 \pmod{p}$, which follows from the p -adic properties of harmonic sums. In [3], Ahlgren and Ono also need an entity similar to $d_{(p-1)/2}$ to be zero modulo p , which they established using a binomial coefficient identity proved by the WZ method [2].

In the above examples, supercongruences of a sequence c_n were shown to be equivalent to congruences of an auxiliary sequence d_n ; and the congruences for d_n were proved using whatever method applied in each case. Similarly, the supercongruence in Theorem 1 for the sequence $a_n = \sum_{i=0}^n \binom{2i}{i}^3 \left(\frac{\lambda}{64}\right)^i$ is equivalent to the auxiliary congruence in Corollary 2 for the sequence $d_n = \sum_{i=0}^n \binom{2i}{i}^3 \left(\frac{\lambda}{64}\right)^i (6(H_{2i} - H_i) + \frac{(\lambda/64)^{p-1}-1}{p})$. However, we proved our supercongruence using the theorem of Coster and Van Hamme, and thus obtain our auxiliary congruence. We know of no direct proof of Corollary 2; we expect a proof for each fixed individual λ might require some combinatorial identity and additional intelligent guesses of WZ pairs to prove the identity, see [1,3].

Lemma 8. For the sequence $a_n = \sum_{i=0}^n \binom{2i}{i}^3 \left(\frac{\lambda}{64}\right)^i$, we introduce the auxiliary sequence $d_n = \sum_{i=0}^n \binom{2i}{i}^3 \left(\frac{\lambda}{64}\right)^i (6(H_{2i} - H_i) + \frac{(\lambda/64)^{p-1}-1}{p})$. Then for any prime p , any k with $\frac{p-1}{2} \leq k < p$, and any n ,

$$a_{k+pn} \equiv a_k a_n + p d_k \sum_{i=0}^n i \binom{2i}{i}^3 \left(\frac{\lambda}{64}\right)^i \pmod{p^2}.$$

Proof. Notice we can write $a_{k+pn} - a_k a_n$ as the telescoping sum $\sum_{i=1}^n T_{k,i}$, where

$$\begin{aligned} T_{k,n} &= (a_{k+pn} - a_k a_n) - (a_{k+p(n-1)} - a_k a_{n-1}) \\ &= (a_{k+pn} - a_{k+p(n-1)}) - a_k (a_n - a_{n-1}) \\ &= \sum_{i=-p+k+1}^k \binom{2i+2pn}{i+pn}^3 \left(\frac{\lambda}{64}\right)^{i+pn} - \left(\sum_{i=0}^k \binom{2i}{i}^3 \left(\frac{\lambda}{64}\right)^i\right) \binom{2n}{n}^3 \left(\frac{\lambda}{64}\right)^n \end{aligned}$$

Using the condition that $\frac{p-1}{2} \leq k < p$, we notice that $\binom{2i+2pn}{i+pn} \equiv 0 \pmod{p}$ if $-p+k+1 < i < 0$. Simplifying modulo p^2 , these terms disappear and we can factor.

$$T_{k,n} \equiv \sum_{i=0}^k \left(\binom{2i+2pn}{i+pn}^3 \left(\frac{\lambda}{64}\right)^{pn} - \binom{2n}{n}^3 \left(\frac{\lambda}{64}\right)^n \binom{2i}{i}^3 \right) \left(\frac{\lambda}{64}\right)^i \pmod{p^2}$$

The factor $\binom{2i+2pn}{i+pn}^3$ may be rewritten as $\frac{-\Gamma_p(1+2i+2pn)^3}{\Gamma_p(1+i+pn)^6} \binom{2n}{n}^3$, where Γ_p is the p -adic Gamma function (see [21, Chapter 11]). Let $T_{k,n} \equiv \left(\frac{\lambda}{64}\right)^n \binom{2n}{n}^3 U_{k,n} \pmod{p^2}$, where

$$U_{k,n} = \sum_{i=0}^k \left(\left(\frac{-\Gamma_p(1+2i+2pn)^3}{\Gamma_p(1+i+pn)^6} \right) \left(\frac{\lambda}{64}\right)^{(p-1)n} - \binom{2i}{i}^3 \right) \left(\frac{\lambda}{64}\right)^i.$$

To simplify the p -adic Gamma function modulo p^2 , we expand Γ_p in terms of factorials and harmonic sums $H_n = \sum_{i=1}^n \frac{1}{i}$. (By convention, $H_0 = 0$.) We also use the congruence, for $p > 3$, that $H_{p-1} \equiv 0 \pmod{p}$. (Wolstenholme has shown this congruence holds modulo p^2 , though we only need modulo p [31].)

$$\begin{aligned} \Gamma_p(1+i+pn)^r &\equiv (-1)^{(1+i+pn)r} i!^r (1+pnrH_i) \prod_{j=0}^{n-1} (p-1)!^r (1+pjrH_{p-1}) \pmod{p^2} \\ &\equiv (-1)^{(1+i+pn)r} i!^r (1+pnrH_i) (-1)^{nr} \pmod{p^2} \\ &\equiv (-1)^{(1+i)r} i!^r (1+pnrH_i) \pmod{p^2} \end{aligned}$$

Plugging this into $U_{k,n}$, we have

$$\begin{aligned} U_{k,n} &\equiv \sum_{i=0}^k \left(\left(\frac{(2i)!^3 (1+6pnH_{2i})}{(i)!^6 (1+6pnH_i)} \right) \left(\frac{\lambda}{64}\right)^{(p-1)n} - \binom{2i}{i}^3 \right) \left(\frac{\lambda}{64}\right)^i \pmod{p^2} \\ &\equiv \sum_{i=0}^k \binom{2i}{i}^3 \left(\frac{\lambda}{64}\right)^i \left((1+6pn(H_{2i} - H_i)) \left(\frac{\lambda}{64}\right)^{(p-1)n} - 1 \right) \pmod{p^2} \end{aligned}$$

$$\text{Using } \left(\frac{\lambda}{64}\right)^{(p-1)n} = \left(1 + p \left(\frac{\left(\frac{\lambda}{64}\right)^{p-1} - 1}{p}\right)\right)^n \equiv 1 + pn \left(\frac{\left(\frac{\lambda}{64}\right)^{p-1} - 1}{p}\right) \pmod{p^2},$$

$$\begin{aligned}
U_{k,n} &\equiv \sum_{i=0}^k \binom{2i}{i}^3 \left(\frac{\lambda}{64}\right)^i \left((1 + 6pn(H_{2i} - H_i)) \left(1 + pn \left(\frac{(\frac{\lambda}{64})^{p-1} - 1}{p} \right) \right) - 1 \right) \\
&\equiv pn \sum_{i=0}^k \binom{2i}{i}^3 \left(\frac{\lambda}{64}\right)^i \left(6(H_{2i} - H_i) + \left(\frac{(\frac{\lambda}{64})^{p-1} - 1}{p} \right) \right) \pmod{p^2}
\end{aligned}$$

So $T_{k,n} \equiv pn \binom{2n}{n}^3 \left(\frac{\lambda}{64}\right)^n d_k \pmod{p^2}$. Combining this congruence with the telescoping sum $a_{k+pn} - a_k a_n = \sum_{i=1}^n T_{k,i}$ completes the proof of the lemma. \square

Using this lemma, we show the equivalence of [Theorem 1](#) and [Corollary 2](#).

Proof of [Corollary 2](#). We consider $T_{k,n}$ with $k = \frac{p-1}{2}$ and $n = 1$. By definition, $T_{\frac{p-1}{2},1} = a_{\frac{3p-1}{2}} - a_{\frac{p-1}{2}} a_{\frac{3-1}{2}}$; we can rewrite this, modulo p^2 , as $P_{\frac{3p-1}{2}}(\sqrt{1-\lambda})^2 - P_{\frac{p-1}{2}}(\sqrt{1-\lambda})^2 P_{\frac{3-1}{2}}(\sqrt{1-\lambda})^2$. Since the sequence $P_{\frac{n-1}{2}}(\sqrt{1-\lambda})$ satisfies ASD congruences, we know that $T_{\frac{p-1}{2},1} \equiv 0 \pmod{p}$. However, [Theorem 1](#) is precisely the information we need to conclude that $T_{\frac{p-1}{2},1} \equiv 0 \pmod{p^2}$ whenever λ is a CM value of E_λ that embeds in \mathbb{Z}_p .

Thus, since

$$T_{\frac{p-1}{2},1} \equiv \frac{p\lambda}{8} \sum_{i=0}^{(p-1)/2} \binom{2i}{i}^3 \left(\frac{\lambda}{64}\right)^i \left(6(H_{2i} - H_i) + \left(\frac{(\frac{\lambda}{64})^{p-1} - 1}{p} \right) \right) \pmod{p^2},$$

we have the desired congruence $d_{\frac{p-1}{2}} \equiv 0 \pmod{p}$ whenever we have supercongruences for $a_{\frac{p-1}{2}}$. \square

Acknowledgments

The paper grew out of the Research Experience for Undergraduates in number theory at Iowa State University, which took place in Fall 2011. It was supported by NSF grant DMS-1001332. A significant part of the work was done while the second author was visiting Cornell University as an AWM Ruth I. Michler fellow. She would like to thank both AWM and Cornell for the excellent opportunity. The authors thank Zhi-Wei Sun for pointing out his papers [\[26,27\]](#), which contain his survey of the subject and many of the conjectures studied here, and for pointing out [\[30\]](#). The authors also thank Ravi Ramakrishna for his helpful comments.

References

- [1] S. Ahlgren, Gaussian hypergeometric series and combinatorial congruences, in: *Symbolic Computation, Number Theory, Special Functions, Physics and Combinatorics*, Gainesville, Florida, 1999, pp. 1–12.
- [2] S. Ahlgren, S. Ekhad, K. Ono, D. Zeilberger, A binomial coefficient identity associated to a conjecture of Beukers, *Electron. J. Combin.* 5 (1998), Research Paper 10, 1 p.

- [3] S. Ahlgren, K. Ono, A Gaussian hypergeometric series evaluation and Apéry number congruences, *J. Reine Angew. Math.* 518 (2000) 187–212.
- [4] S. Ahlgren, K. Ono, D. Penniston, Zeta functions of an infinite family of K3 surfaces, *Amer. J. Math.* 124 (2) (Apr. 2002) 353–368.
- [5] G. Andrews, R. Askey, R. Roy, *Special Functions*, Encyclopedia Math. Appl., vol. 71, Cambridge University Press, Cambridge, 1999, xvi+664 pp.
- [6] A.O.L. Atkin, H.P.F. Swinnerton-Dyer, Modular forms on noncongruence subgroups, in: *Proc. Sympos. Pure Math.*, vol. 19, Amer. Math. Soc., Providence, RI, 1971, pp. 1–25.
- [7] H.H. Chan, L. Long, W. Zudilin, A supercongruence motivated by the Legendre family of elliptic curves, *Russ. Math. Notes* 88 (3–4) (2010) 599–602.
- [8] S. Chisholm, A. Deines, L. Long, G. Nebe, H. Swisher, p -Adic analogues of Ramanujan type formulas for $1/\pi$, *Mathematics* 1 (1) (2013) 9–30.
- [9] M.J. Coster, L. van Hamme, Supercongruences of Atkin and Swinnerton-Dyer type for Legendre polynomials, *J. Number Theory* 38 (1991) 265–286.
- [10] M. Deuring, Die Typen der Multiplikatorringe elliptischer Funktionenkörper, *Abh. Math. Sem. Hansischen Univ.* 14 (1941) 197–272 (in German).
- [11] B. Dwork, p -adic cycles, *Publ. Math. Inst. Hautes Études Sci.* 37 (1969) 27–115.
- [12] I. Gessel, Some congruences for Apéry numbers, *J. Number Theory* 14 (1982) 362–368.
- [13] T. Ishikawa, On Beuker’s conjecture, *Kobe J. Math.* 6 (1) (1989) 49–51.
- [14] T. Ishikawa, Super congruence for the Apéry numbers, *Nagoya Math. J.* 118 (1990) 195–202.
- [15] T. Kilbourn, An extension of the Apéry number supercongruence, *Acta Arith.* 123 (4) (2006) 335–348.
- [16] W.W. Li, L. Long, Fourier coefficients of noncongruence cuspforms, *Bull. Lond. Math. Soc.* 44 (3) (2012) 591–598.
- [17] L. Long, On a Shioda–Inose structure of a family of K3 surfaces, in: *Calabi–Yau Varieties and Mirror Symmetry*, Toronto, ON, 2001, in: *Fields Inst. Commun.*, vol. 38, Amer. Math. Soc., Providence, RI, 2003, pp. 201–207.
- [18] L. Long, Hypergeometric evaluation identities and supercongruences, *Pacific J. Math.* 249 (2) (2011) 405–418.
- [19] L. Long, R. Ramakrishna, Some supercongruences occurring in truncated hypergeometric series, *Adv. Math.* 290 (2016) 773–808.
- [20] D. McCarthy, Extending Gaussian hypergeometric series to the p -adic setting, *Int. J. Number Theory* 8 (7) (2012) 1581–1612.
- [21] K. Ono, The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q -Series, CBMS Reg. Conf. Ser. Math., vol. 102, American Mathematical Society, Providence, RI, 2004, viii+216 pp. Published for the Conference Board of the Mathematical Sciences, Washington, DC.
- [22] F. Rodriguez-Villegas, Hypergeometric families of Calabi–Yau manifolds, in: *Calabi–Yau Varieties and Mirror Symmetry*, Toronto, ON, 2001, in: *Fields Inst. Commun.*, vol. 38, Amer. Math. Soc., Providence, RI, 2003, pp. 223–231.
- [23] A.J. Scholl, Modular forms and de Rham cohomology; Atkin–Swinnerton-Dyer congruences, *Invent. Math.* 79 (1) (1985) 49–77.
- [24] J. Stienstra, Formal group laws arising from algebraic varieties, *Amer. J. Math.* 109 (5) (1987) 907–925.
- [25] J. Stienstra, F. Beukers, On the Picard–Fuchs equation and the formal Brauer group of certain elliptic K3-surfaces, *Math. Ann.* 271 (2) (1985) 269–304.
- [26] Z.-W. Sun, Super congruences and Euler numbers, *Sci. China Math.* 54 (2011) 2509–2535.
- [27] Z.-W. Sun, Determining x or $y \bmod p^2$ with $x^2 + dy^2 = p$, arXiv:1210.5237, 2012.
- [28] Z.-H. Sun, Congruences concerning Legendre polynomials II, *J. Number Theory* 133 (6) (2013) 1950–1976.
- [29] L. Van Hamme, Proof of a conjecture of Beukers on Apéry numbers, in: N. De Grande-De Kimpe, L. Van Hamme (Eds.), *Proceedings of the Conference on p -Adic Analysis*, Hengelhoeft, 1986, pp. 189–195.
- [30] L. Van Hamme, Some conjectures concerning partial sums of generalized hypergeometric series, in: *p -Adic Functional Analysis*, Nijmegen, 1996, in: *Lect. Notes Pure Appl. Math.*, vol. 192, Dekker, New York, 1997, pp. 223–236.
- [31] J. Wolstenholme, On certain properties of prime numbers, *Q. J. Pure Appl. Math.* 5 (1862) 35–39.