ACTA ARITHMETICA
123.4 (2006)

An extension of the Apéry number supercongruence

by

Timothy Kilbourn (Urbana, IL)

1. Introduction and statement of results. Let

$$f(z) := \eta^4(2z)\eta^4(4z) = q\prod_{n=1}^{\infty}(1-q^{2n})^4(1-q^{4n})^4 = \sum_{n=1}^{\infty} a(n)q^n \tag{1.1}$$

be the unique normalized eigenform in the space $S_4(\Gamma_0(8))$ of weight four cuspforms on the congruence subgroup $\Gamma_0(8)$, where $q := e^{2\pi iz}$ and

$$\eta(z) := q^{\frac{1}{24}}\prod_{n=1}^{\infty}(1-q^n)$$

is Dedekind's eta function. In [4], Beukers proved that for odd primes p,

$$a(p) \equiv A\left(\frac{p-1}{2}\right) \pmod{p}, \tag{1.2}$$

where $A(n)$ is the Apéry number

$$A(n) := \sum_{j=0}^{n}\binom{n+j}{j}^2\binom{n}{j}^2.$$

He conjectured that in fact

$$a(p) \equiv A\left(\frac{p-1}{2}\right) \pmod{p^2}. \tag{1.3}$$

This was proved for primes p such that $p \nmid a(p)$ by Ishikawa [8] and unconditionally by Ahlgren and Ono [1].

The $a(p)$ for odd primes p are also known to be related to the modular Calabi–Yau threefold

$$x + \frac{1}{x} + y + \frac{1}{y} + z + \frac{1}{z} + w + \frac{1}{w} = 0, \tag{1.4}$$

in the following way. Let $N(p)$ denote the number of solutions to (1.4) over the finite field with p elements. Then Ahlgren and Ono [2], van Geemen and

2000 *Mathematics Subject Classification*: Primary 11F33; Secondary 11S80.

Nygaard [6], and Verrill [14] proved by different methods that

$$a(p) = p^3 - 2p^2 - 7 - N(p) \tag{1.5}$$

for odd primes p. This also allows Ahlgren and Ono to give a representation of $a(p)$ in terms of Gaussian hypergeometric series, the finite field analogs of the classical hypergeometric series.

In [13], Rodriguez-Villegas considers hypergeometric weight systems of the form

$$\gamma = \sum_{k=1}^{\infty} \gamma_k [k],$$

where $\gamma_k = 0$ for all but finitely many k, satisfying the two conditions:

(1) $\displaystyle\sum_{k=1}^{\infty} k\gamma_k = 0,$

(2) $\displaystyle d = d(\gamma) := -\sum_{k=1}^{\infty} \gamma_k > 0.$

The integer d is called the *dimension* of γ. To such a γ we may associate a hypergeometric function

$$u(\lambda) := \sum_{n=0}^{\infty} u_n \lambda^n \quad \text{where} \quad u_n = \prod_{k=1}^{\infty} (kn)!^{\gamma_k}.$$

This function $u(\lambda)$ satisfies an order r linear differential equation, and r is called the *rank* of γ.

Rodriguez-Villegas shows that in the case where $d = r$, the coefficients u_n are integers for all n, so the truncation

$$\sum_{n=0}^{p-1} u_n \lambda^n \bmod p$$

is well defined. When $d = r = 4$, there is a family of Calabi–Yau threefolds associated to γ via toric geometry. For a certain value $\lambda = \lambda_0$, Rodriguez-Villegas observed that numerically,

$$\sum_{n=0}^{p-1} u_n \lambda_0^n \equiv c(p) \pmod{p^3}$$

for primes p not dividing λ_0^{-1}, where the $c(p)$ are the coefficients of a weight four modular form depending on γ. If $\gamma = 4[2] - 8[1]$, then $\lambda_0 = 2^{-8}$, the modular form is $f(z)$, and we prove Rodriguez-Villegas' observation in the following theorem.

THEOREM 1. *Let p be an odd prime, and let $a(p)$ be defined as in* (1.1). *Then*

$$a(p) \equiv \sum_{j=0}^{p-1} \binom{2j}{j}^4 2^{-8j} \pmod{p^3}.$$

Note that by combining Lemma 4.5 below and [1, Lemma 7.2], this theorem extends Beukers' supercongruence (1.3). For hypergeometric weight systems with dimension and rank equal to 2, Rodriguez-Villegas obtains a family of elliptic curves, and similar mod p^2 supercongruences hold. These have been proved by Mortenson ([10]–[12]).

The crucial ingredient in the proof of Theorem 1 is the fact that the Calabi–Yau threefold (1.4) is modular. By using character sums to calculate the quantity $N(p)$, we can write $a(p)$ in terms of character sums using (1.5), as in [1, Theorem 6]. The Gross–Koblitz formula then transforms the character sums into expressions involving the p-adic gamma function.

The modularity result allows us to relate the Calabi–Yau threefold to the modular form $f(z)$. For the other threefolds listed in [13], it seems likely that a similar modularity result would allow us to apply the techniques in this paper. It is possible that another approach could also provide a connection between the modular forms and the hypergeometric series. For example, by the work of Deligne, we know that the coefficients of these modular forms are related to certain 2-dimensional Galois representations; it would be interesting to see if these representations can be related directly to the hypergeometric series in question.

Also, Theorem 1 does not hold modulo p^4. A similar analysis could probably be carried out modulo p^4, but the expressions involved would be considerably more complicated.

In Section 2, we will review some properties of the p-adic gamma function and its logarithmic derivatives. In Section 3 we use the Gross–Koblitz formula to reduce the proof of Theorem 1 to the proof of Proposition 3.1. In Section 4 we use properties of the p-adic gamma function to prove Proposition 3.1.

2. p-adic preliminaries. Let p be an odd prime. Throughout the paper, $|\cdot|$ denotes the p-adic absolute value on $\mathbb{Q}_p$, normalized so that $|p| = p^{-1}$. We recall the definition of the p-adic gamma function on the p-adic integers $\mathbb{Z}_p$ (see [9, Ch. IV] for details). For integers $n \in \mathbb{N}$, set

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

and extend to all $x \in \mathbb{Z}_p$ by setting

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

It is known that this limit exists, and it is independent of the sequence of integers approaching x p-adically. This function is locally analytic and has a Taylor series expansion (see [5])

$$\Gamma_p(x+z) = \sum_{n=0}^{\infty} a_n z^n, \qquad a_n \in \mathbb{Q}_p, \tag{2.1}$$

with radius of convergence

$$\varrho := p^{-\frac{1}{p} - \frac{1}{p-1}}.$$

The following proposition gives some basic properties of Γ_p and is an easy consequence of the definition of $\Gamma_p(x)$ (see, e.g., [9]).

Proposition 2.1. *Let $n \in \mathbb{N}$ and $x \in \mathbb{Z}_p$. Then*

(1) $\Gamma_p(0) = 1$.
(2) $\dfrac{\Gamma_p(x+1)}{\Gamma_p(x)} = \begin{cases} -x & \text{if } |x| = 1, \\ -1 & \text{if } |x| < 1. \end{cases}$
(3) $|\Gamma_p(x)| = 1$.
(4) *Let $x_0 \in \{1, \ldots, p\}$ be the constant term in the p-adic expansion of x. Then $\Gamma_p(x)\Gamma_p(1-x) = (-1)^{x_0}$.*
(5) *If $x \equiv y \pmod{p^n}$, then $\Gamma_p(x) \equiv \Gamma_p(y) \pmod{p^n}$.*

Now we consider the logarithmic derivative of Γ_p. For $x \in \mathbb{Z}_p$, let

$$G_1(x) := \frac{\Gamma_p'(x)}{\Gamma_p(x)}, \qquad G_2(x) := \frac{\Gamma_p''(x)}{\Gamma_p(x)}.$$

By the local analyticity of $\Gamma_p(x)$ and the fact that $|\Gamma_p(x)| = 1$, these functions are defined on all of $\mathbb{Z}_p$.

Proposition 2.2. *Let $x \in \mathbb{Z}_p^{\times}$. Then*

(1) $G_1(x+1) - G_1(x) = 1/x$.
(2) $G_2(x+1) - G_2(x) = G_1(x+1)^2 - G_1(x)^2 - 1/x^2$.

Proof. We obtain the first assertion from Proposition 2.1(2), and the second assertion is obtained by differentiating the first. ∎

Next we discuss some congruence properties of the p-adic gamma function and its derivatives. Our arguments follow the work of Chowla, Dwork, and Evans [5].

PROPOSITION 2.3. *Let $p \geq 7$ be prime, $x \in \mathbb{Z}_p$, and $z \in p\mathbb{Z}_p$. Then*

(1) $G_1(x), G_2(x) \in \mathbb{Z}_p$.

(2)

$$\mathit{\Gamma}_p(x+z) \equiv \mathit{\Gamma}_p(x)\left(1 + zG_1(x) + \frac{z^2}{2} G_2(x)\right) \pmod{p^3}. \tag{2.2}$$

(3)

$$\mathit{\Gamma}_p'(x+z) \equiv \mathit{\Gamma}_p'(x) + z\mathit{\Gamma}_p''(x) \pmod{p^2}. \tag{2.3}$$

Proof. Recall the Taylor series expansion (2.1) for $\mathit{\Gamma}_p(x+z)$ with radius $\varrho = p^{-1/p-1/(p-1)}$. We know that $|a_n| \leq \varrho^{-n}$ for $n = 0, 1, \ldots$. If $p \geq 2n+1$, then $\varrho^{-n} < p$. Since $a_n \in \mathbb{Q}_p$, we have

$$|a_n| \leq 1 \quad \text{ if } p \geq 2n+1. \tag{2.4}$$

By (2.1), $a_n = (1/n!)\mathit{\Gamma}_p^{(n)}(x)$, where $\mathit{\Gamma}_p^{(n)}(x)$ is the nth derivative of $\mathit{\Gamma}_p$ at x. Now for $n = 1, 2$, we have

$$|G_n(x)| = \frac{|\mathit{\Gamma}_p^{(n)}(x)|}{|\mathit{\Gamma}_p(x)|} = |\mathit{\Gamma}_p^{(n)}(x)| = |n!a_n|,$$

since by Proposition 2.1 we have $|\mathit{\Gamma}_p(x)| = 1$. Thus for $p \geq 5$ we have $G_1(x), G_2(x) \in \mathbb{Z}_p$.

If $|z| \leq |p|$, then

$$|a_n z^n| \leq \frac{|p|^n}{\varrho^n} = |p|^{n(1-\frac{1}{p}-\frac{1}{p-1})}.$$

Since $a_n \in \mathbb{Q}_p$, we can conclude that

$$a_n z^n \equiv 0 \pmod{p^{\beta_n}},$$

where β_n is the smallest integer such that

$$\beta_n \geq n\left(1 - \frac{1}{p} - \frac{1}{p-1}\right).$$

If $n \geq 4$ and $p \geq 5$, then $\beta_n \geq \beta_4 \geq 3$, so

$$\mathit{\Gamma}_p(x+z) \equiv a_0 + a_1 z + a_2 z^2 + a_3 z^3 \pmod{p^3}.$$

For $p \geq 7$, by (2.4) we see that $a_3 \in \mathbb{Z}_p$ and

$$\mathit{\Gamma}_p(x+z) \equiv a_0 + a_1 z + a_2 z^2 \pmod{p^3}$$

since $|z| \leq |p|$. Now (2.2) follows since $a_i = (1/i!)\mathit{\Gamma}_p^{(i)}(x)$.

For (2.3), note that

$$\mathit{\Gamma}_p'(x+z) = \sum_{n=0}^{\infty} n a_n z^{n-1},$$

where the a_n are as in (2.1). Thus the same arguments can be used to prove (2.3). ∎

3. Proof of Theorem 1. The cases $p=3$ and $p=5$ can be checked explicitly, so assume $p \geq 7$. Let ϕ be the quadratic character on $\mathbb{F}_p^\times$. From [1, Lemma 7.1], we know that

$$a(p) = \frac{-1}{p-1} \sum_{\chi} J(\phi,\chi)^4 - p, \tag{3.1}$$

where $J(\phi,\chi)$ is the Jacobi sum of the $\mathbb{F}_p^\times$-characters ϕ and χ, and the sum runs over all such characters χ. By using basic properties of Jacobi sums and Gauss sums $g(\chi)$ (see [3]), we can write

$$\sum_{\chi} J(\phi,\chi)^4 = 1 + p^2 \sum_{\chi\neq\phi} \frac{g(\chi)^4}{g(\phi\chi)^4}.$$

We can consider the characters χ as taking values in $\mathbb{Z}_p^\times$, and hence $g(\chi) \in \mathbb{C}_p$. Let $\pi \in \mathbb{C}_p$ be a fixed root of $x^{p-1}+p=0$. If we let ω be the Teichmüller character, then the Gross–Koblitz formula [7] states that with an appropriate normalization of the Gauss sum,

$$g(\omega^{-j}) = -\pi^j \Gamma_p\left(\frac{j}{p-1}\right), \qquad 0 \leq j \leq p-2.$$

Applying this to our present situation, we can write (as in [1])

$$\begin{aligned}
\sum_{\chi} J(\phi,\chi)^4 &= 1 + p^2 \sum_{j=0}^{(p-3)/2} \frac{g(\omega^{-j})^4}{g(\phi\omega^{-j})^4} + p^2 \sum_{j=(p+1)/2}^{p-2} \frac{g(\omega^{-j})^4}{g(\phi\omega^{-j})^4} \\
&= 1 + p^2 \sum_{j=0}^{(p-3)/2} \frac{g(\omega^{-j})^4}{g(\omega^{-(j+\frac{p-1}{2})})^4} + p^2 \sum_{j=(p+1)/2}^{p-2} \frac{g(\omega^{-j})^4}{g(\omega^{-(j-\frac{p-1}{2})})^4} \\
&= 1 + \sum_{j=0}^{(p-3)/2} \frac{\Gamma_p\big(\frac{j}{p-1}\big)^4}{\Gamma_p\big(\frac{j}{p-1}+\frac{1}{2}\big)^4} + p^4 \sum_{j=(p+1)/2}^{p-2} \frac{\Gamma_p\big(\frac{j}{p-1}\big)^4}{\Gamma_p\big(\frac{j}{p-1}-\frac{1}{2}\big)^4}.
\end{aligned}$$

We combine this with (3.1) to see that

$$\begin{aligned}
a(p) &\equiv \frac{-1}{p-1}\left(1 + \sum_{j=0}^{(p-3)/2} \frac{\Gamma_p\big(\frac{j}{p-1}\big)^4}{\Gamma_p\big(\frac{j}{p-1}+\frac{1}{2}\big)^4}\right) - p \\
&\equiv p^2+1+(p^2+p+1) \sum_{j=0}^{(p-3)/2} \frac{\Gamma_p\big(\frac{j}{p-1}\big)^4}{\Gamma_p\big(\frac{j}{p-1}+\frac{1}{2}\big)^4} \pmod{p^3}.
\end{aligned}$$

We have $j/(p-1) \equiv -j-jp-jp^2 \pmod{p^3}$, so Proposition (2.1)(5) gives

$$a(p) \equiv p^2+1+(p^2+p+1) \sum_{j=0}^{(p-3)/2} \frac{\Gamma_p(-j-jp-jp^2)^4}{\Gamma_p(1/2-j-jp-jp^2)^4} \pmod{p^3}.$$

Applying Proposition 2.1(4) and reindexing the summation, we have

$$a(p) \equiv p^2+1+(p^2+p+1) \sum_{j=1}^{(p-1)/2} \frac{\Gamma_p(1/2+j+jp+jp^2)^4}{\Gamma_p\,(1+j+jp+jp^2)^4} \pmod{p^3}. \tag{3.2}$$

By Proposition 2.3, we see that

$$\begin{aligned}\Gamma_p(x_0+j+jp+jp^2)^4 \equiv \Gamma_p(x_0+j)^4[1+4(jp+jp^2)G_1(x_0+j) \\ +(jp+jp^2)^2(2G_2(x_0+j)+6G_1(x_0+j)^2)] \pmod{p^3}\end{aligned} \tag{3.3}$$

for $x_0 \in \mathbb{Z}_p$. We expand the numerator and denominator of (3.2) with $x_0 = 1/2$ and $x_0 = 1$ respectively. By multiplying the numerator and denominator by

$$1-4jpG_1(1+j)-2j^2p^2(G_2(1+j)-5G_1(1+j)^2)-4jp^2G_1(1+j),$$

we conclude that

$$\begin{aligned}a(p) \equiv p^2+1+(p^2+p+1) \sum_{j=1}^{(p-1)/2} \frac{\Gamma_p\left(\frac{1}{2}+j\right)^4}{\Gamma_p(1+j)^4}\,(1+4jpA(j) \\ +4jp^2A(j)+2j^2p^2B(j)) \pmod{p^3},\end{aligned} \tag{3.4}$$

where

$$A(j) := G_1\left(\tfrac{1}{2}+j\right)-G_1(1+j) \tag{3.5}$$

and

$$\begin{aligned}B(j) := G_2\left(\tfrac{1}{2}+j\right)-G_2(1+j)+3G_1\left(\tfrac{1}{2}+j\right)^2 \\ +5G_1(1+j)^2-8G_1\left(\tfrac{1}{2}+j\right)G_1(1+j).\end{aligned} \tag{3.6}$$

Now define

$$X(p) := 1+\sum_{j=1}^{(p-1)/2} \frac{\Gamma_p\left(\frac{1}{2}+j\right)^4}{\Gamma_p(1+j)^4}\,(1+8jA(j)+2j^2B(j)), \tag{3.7}$$

$$Y(p) := \sum_{j=1}^{(p-1)/2} \frac{\Gamma_p\left(\frac{1}{2}+j\right)^4}{\Gamma_p(1+j)^4}\,(1+4jA(j)), \tag{3.8}$$

$$Z(p) := 1+\sum_{j=1}^{(p-1)/2} \frac{\Gamma_p\left(\frac{1}{2}+j\right)^4}{\Gamma_p(1+j)^4}. \tag{3.9}$$

By grouping the terms in (3.4) according to powers of p, we obtain

$$a(p) \equiv p^2X(p)+pY(p)+Z(p) \pmod{p^3}.$$

Thus Theorem 1 is proved on account of the following proposition, which will be proved in the next section.

PROPOSITION 3.1. *Let $p \geq 7$ be prime, and let $X(p)$, $Y(p)$, and $Z(p)$ be defined as in* (3.7), (3.8), *and* (3.9). *Then*

(1) $X(p) \equiv 0 \pmod{p}$.
(2) $Y(p) \equiv 0 \pmod{p^2}$.
(3) $Z(p) \equiv \sum_{j=0}^{(p-1)/2} \binom{2j}{j}^4 2^{-8j} \pmod{p^3}$.

4. Proof of Proposition 3.1. We will now examine the terms $X(p)$, $Y(p)$, and $Z(p)$ individually to prove Proposition 3.1. First we make some definitions that will be useful in what follows.

For $i, n \in \mathbb{N}$, we define the generalized harmonic sums $H_n^{(i)}$ as

$$H_n^{(i)} := \sum_{j=1}^{n} \frac{1}{j^i}. \tag{4.1}$$

Also for integers γ we define

$$(\gamma)_n := \begin{cases} 1 & \text{if } n = 0, \\ \gamma(\gamma+1)(\gamma+2)\cdots(\gamma+n-1) & \text{if } n \geq 1. \end{cases}$$

We first consider $X(p)$. We have

$$\begin{aligned} X(p) = 1 &+ \sum_{j=1}^{(p-1)/2} \frac{\Gamma_p\left(\frac{1}{2}+j\right)^4}{\Gamma_p(1+j)^4} (1 + 4jA(j)) \\ &+ \sum_{j=1}^{(p-1)/2} \frac{\Gamma_p\left(\frac{1}{2}+j\right)^4}{\Gamma_p(1+j)^4} (4jA(j) + 2j^2 B(j)). \end{aligned}$$

Ahlgren and Ono proved in [1, Lemma 7.3] that

$$\sum_{j=1}^{(p-1)/2} \frac{\Gamma_p\left(\frac{1}{2}+j\right)^4}{\Gamma_p(1+j)^4} (1 + 4jA(j)) \equiv 0 \pmod{p},$$

so in order to prove the first assertion of Proposition 3.1, we need to show that

$$1 + \sum_{j=1}^{(p-1)/2} \frac{\Gamma_p\left(\frac{1}{2}+j\right)^4}{\Gamma_p(1+j)^4} (4jA(j) + 2j^2 B(j)) \equiv 0 \pmod{p}. \tag{4.2}$$

We will use the following lemmas.

LEMMA 4.1. *Let p be an odd prime and $0 \leq j \leq (p-1)/2$. Let $A(j)$ and $B(j)$ be defined as in* (3.5) *and* (3.6). *Then*

$$A(j) \equiv H^{(1)}_{(p-1)/2+j} - H^{(1)}_j + 2p \sum_{r=0}^{j-1} \frac{1}{(2r+1)^2} \pmod{p^2} \tag{4.3}$$

and

$$B(j) \equiv 4(H^{(1)}_{(p-1)/2+j} - H^{(1)}_j)^2 - (H^{(2)}_{(p-1)/2+j} - H^{(2)}_j) \pmod{p}. \tag{4.4}$$

Proof. We begin by proving (4.3). By Proposition 2.3, we see that

$$\begin{aligned} G_1\left(\tfrac{1}{2}+j\right) &= \frac{\Gamma_p'\left(\frac{1}{2}+j\right)}{\Gamma_p\left(\frac{1}{2}+j\right)} \\ &\equiv \frac{\Gamma_p'\left(\frac{p+1}{2}+j\right) - \frac{p}{2}\Gamma_p''\left(\frac{1}{2}+j\right)}{\Gamma_p\left(\frac{p+1}{2}+j\right) - \frac{p}{2}\Gamma_p'\left(\frac{1}{2}+j\right)} \\ &\equiv \frac{\Gamma_p'\left(\frac{p+1}{2}+j\right)}{\Gamma_p\left(\frac{p+1}{2}+j\right)} + \frac{p}{2}\,\frac{\Gamma_p'\left(\frac{1}{2}+j\right)\Gamma_p'\left(\frac{p+1}{2}+j\right)}{\Gamma_p\left(\frac{p+1}{2}+j\right)^2} \\ &\quad - \frac{p}{2}\,\frac{\Gamma_p''\left(\frac{1}{2}+j\right)}{\Gamma_p\left(\frac{p+1}{2}+j\right)} \pmod{p^2}. \end{aligned}$$

By Proposition 2.3, we have

$$\Gamma_p'\left(\frac{p+1}{2}+j\right) \equiv \Gamma_p'\left(\frac{1}{2}+j\right) \pmod{p},$$

and a similar argument shows that

$$\Gamma_p''\left(\frac{p+1}{2}+j\right) \equiv \Gamma_p''\left(\frac{1}{2}+j\right) \pmod{p}. \tag{4.5}$$

We see that

$$\begin{aligned} &G_1\left(\frac{1}{2}+j\right) \\ &\equiv G_1\left(\frac{p+1}{2}+j\right) + \frac{p}{2}\left(G_1\left(\frac{1}{2}+j\right)^2 - G_2\left(\frac{1}{2}+j\right)\right) \pmod{p^2}. \end{aligned} \tag{4.6}$$

Applying Proposition 2.2(2), we can write

$$G_1\left(\frac{1}{2}+j\right)^2 - G_2\left(\frac{1}{2}+j\right) = 4\sum_{r=0}^{j-1} \frac{1}{(2r+1)^2} + G_1\left(\frac{1}{2}\right)^2 - G_2\left(\frac{1}{2}\right). \tag{4.7}$$

If we subtract $G_1(1+j)$ from (4.6), apply (4.7), and repeatedly apply the first assertion of Proposition 2.2, we obtain

$$\begin{aligned} A(j) &\equiv H^{(1)}_{(p-1)/2+j} - H^{(1)}_j \\ &\quad + 2p\left(\sum_{r=0}^{j-1} \frac{1}{(2r+1)^2} + G_1\left(\frac{1}{2}\right)^2 - G_2\left(\frac{1}{2}\right)\right) \pmod{p^2}. \end{aligned}$$

It remains to show that

$$G_1\left(\frac{1}{2}\right)^2 - G_2\left(\frac{1}{2}\right) \equiv 0 \pmod{p}. \tag{4.8}$$

As in Proposition 2.3, we see that

$$\frac{\Gamma_p\left(\frac{1}{2} \pm \frac{p}{2}\right)}{\Gamma_p\left(\frac{1}{2}\right)} \equiv 1 \pm \frac{p}{2} G_1\left(\frac{1}{2}\right) + \frac{p^2}{8} G_2\left(\frac{1}{2}\right) \pmod{p^3}.$$

By multiplying the two terms together we have

$$\frac{\Gamma_p\left(\frac{1}{2} - \frac{p}{2}\right)\Gamma_p\left(\frac{1}{2} + \frac{p}{2}\right)}{\Gamma_p\left(\frac{1}{2}\right)^2} \equiv 1 - \frac{p^2}{4}\left(G_1\left(\frac{1}{2}\right)^2 - G_2\left(\frac{1}{2}\right)\right) \pmod{p^3}. \tag{4.9}$$

Proposition 2.1 shows us that

$$\Gamma_p\left(\frac{1}{2} + \frac{p}{2}\right)\Gamma_p\left(1 - \left(\frac{1}{2} + \frac{p}{2}\right)\right) = (-1)^{(p+1)/2}$$

and

$$\Gamma_p\left(\frac{1}{2}\right)^2 = (-1)^{(p+1)/2}, \tag{4.10}$$

so the left hand side of (4.9) is equal to 1. This proves (4.8), and with it (4.3).

We now turn to the proof of (4.4). By (4.5) and Proposition 2.3 we obtain

$$G_2\left(\frac{p+1}{2} + j\right) \equiv G_2\left(\frac{1}{2} + j\right) \pmod{p},$$

so with Proposition 2.2 we have

$$\begin{aligned} G_2\left(\frac{1}{2} + j\right) &- G_2(1+j) \\ &\equiv G_1\left(\frac{1}{2} + j\right)^2 - G_1(1+j)^2 - (H^{(2)}_{(p-1)/2+j} - H^{(2)}_j) \pmod{p}. \end{aligned}$$

Thus by (3.6) and (4.3), we have

$$\begin{aligned} B(j) &\equiv 4A(j)^2 - (H^{(2)}_{(p-1)/2+j} - H^{(2)}_j) \\ &\equiv 4(H^{(1)}_{(p-1)/2+j} - H^{(1)}_j)^2 - (H^{(2)}_{(p-1)/2+j} - H^{(2)}_j) \pmod{p}. \ \blacksquare \end{aligned}$$

Lemma 4.2. *Let p be an odd prime and $0 \le j \le (p-1)/2$. Then*

$$\frac{\Gamma_p\left(\frac{1}{2} + j\right)^4}{\Gamma_p(1+j)^4} \equiv (j+1)^4_{(p-1)/2} \pmod{p}.$$

Proof. Note that

$$\binom{\frac{p-1}{2}+j}{j}^4 = \frac{\left(\frac{p-1}{2}+j\right)!^4}{j!^4\left(\frac{p-1}{2}\right)!^4} \equiv \frac{\Gamma_p\left(\frac{1}{2}+j\right)^4}{\Gamma_p(1+j)^4} \pmod{p}$$

by Proposition 2.1 and (4.10). The lemma follows since

$$\binom{\frac{p-1}{2}+j}{j}^4 \equiv (j+1)_{(p-1)/2}^4 \pmod{p}. \ \blacksquare$$

Combining these lemmas, we see that to prove (4.2), it is enough to show that

$$\begin{aligned} 1+\sum_{j=1}^{(p-1)/2} (j+1)_{(p-1)/2}^4 (4j(H_{(p-1)/2+j}^{(1)} - H_j^{(1)}) \\ + 8j^2(H_{(p-1)/2+j}^{(1)} - H_j^{(1)})^2 - 2j^2(H_{(p-1)/2+j}^{(2)} - H_j^{(2)})) \equiv 0 \pmod{p}. \end{aligned} \tag{4.11}$$

Let

$$P(z) := \frac{z}{2}\frac{d^2}{dz^2}[z(z+1)_{(p-1)/2}^4] = \sum_{k=0}^{2p-2} a_k z^k, \tag{4.12}$$

with integers a_k.

By a computation, we have

$$\begin{aligned} P(j) \equiv (j+1)_{(p-1)/2}^4 (4j(H_{(p-1)/2+j}^{(1)} - H_j^{(1)}) \\ + 8j^2(H_{(p-1)/2+j}^{(1)} - H_j^{(1)})^2 - 2j^2(H_{(p-1)/2+j}^{(2)} - H_j^{(2)})) \pmod{p}. \end{aligned} \tag{4.13}$$

Combining (4.11) and (4.13) we see that it is enough to show that

$$1+\sum_{j=1}^{(p-1)/2} P(j) \equiv 0 \pmod{p}. \tag{4.14}$$

Note that $(j+1)_{(p-1)/2}$ is divisible by p for $(p-1)/2 < j < p$, and $H_{(p-1)/2+j}^{(i)} - H_j^{(i)} \in (1/p^i)\mathbb{Z}_p$ for $i = 1,2$, so that $P(j) \equiv 0 \pmod{p}$ for such j. Therefore (4.14), and with it the first assertion of Proposition 3.1, will be established after the following lemma whose proof is based on an idea used by Mortenson in [12].

LEMMA 4.3. *Let p be an odd prime and let $P(z)$ be the polynomial defined in* (4.12). *Then*

$$1+\sum_{j=1}^{p-1} P(j) \equiv 0 \pmod{p}.$$

Proof. We recall the following fact about exponential sums modulo p: for k a positive integer, we have

$$\sum_{j=1}^{p-1} j^k \equiv \begin{cases} -1 \pmod p & \text{if } (p-1)\mid k, \\ 0 \pmod p & \text{otherwise.} \end{cases} \tag{4.15}$$

Since $z \mid P(z)$, we have $a_0 = 0$. By applying (4.15), we see that

$$\sum_{j=1}^{p-1} P(j) = \sum_{j=1}^{p-1}\sum_{k=1}^{2p-2} a_k j^k = \sum_{k=1}^{2p-2} a_k \sum_{j=1}^{p-1} j^k \equiv -a_{p-1} - a_{2p-2} \pmod p.$$

Since $P(z)$ is z times a second derivative, we see that $a_{p-1} \equiv 0 \pmod p$. Now write

$$P(z) = \frac{z}{2}\frac{d^2}{dz^2}[z^{2p-1} + \cdots] = \frac{z}{2}((2p-1)(2p-2)z^{2p-3} + \cdots),$$

so $a_{2p-2} \equiv 1 \pmod p$. This proves Lemma 4.3, and so establishes that $X(p) \equiv 0 \pmod p$. ∎

Next we consider $Y(p)$. By (3.8) and Lemma 4.1, we have

$$\begin{aligned} Y(p) &\equiv \sum_{j=1}^{(p-1)/2} \frac{\Gamma_p\left(\frac{1}{2}+j\right)^4}{\Gamma_p(1+j)^4} \\ &\quad \times \left(1 + 4j(H^{(1)}_{(p-1)/2+j} - H^{(1)}_j) + 8jp\sum_{r=0}^{j-1}\frac{1}{(2r+1)^2}\right) \pmod{p^2}. \end{aligned} \tag{4.16}$$

The following lemma reduces $Y(p)$ to an expression involving Γ_p and $H^{(1)}_n$.

LEMMA 4.4. *Let p be an odd prime and $0 \le j \le (p-1)/2$. Then*

$$2j(H^{(1)}_{(p-1)/2+j} - H^{(1)}_{(p-1)/2-j}) \equiv -8jp\sum_{r=0}^{j-1}\frac{1}{(2r+1)^2} \pmod{p^2}.$$

Proof. By pairing terms of the sum, we see that

$$\begin{aligned} H^{(1)}_{(p-1)/2+j} - H^{(1)}_{(p-1)/2-j} &= \frac{1}{\frac{p-1}{2} - j + 1} + \cdots + \frac{1}{\frac{p-1}{2}} + \frac{1}{\frac{p+1}{2}} + \cdots + \frac{1}{\frac{p-1}{2} + j} \\ &= \sum_{r=0}^{j-1} \frac{1}{\frac{p-1}{2} + 1 + r} + \frac{1}{\frac{p-1}{2} - r} = \sum_{r=0}^{j-1}\frac{4p}{p^2 - (2r+1)^2}. \end{aligned}$$

Reducing modulo p^2 and multiplying by $2j$ gives the desired expression. ∎

In the proof of [1, Lemma 7.2], the analysis holds term-by-term, giving

$$\frac{\Gamma_p\left(\frac{1}{2}+j\right)^4}{\Gamma_p(1+j)^4} \equiv \binom{\frac{p-1}{2}+j}{j}^2 \binom{\frac{p-1}{2}}{j}^2 \pmod{p^2}. \tag{4.17}$$

By combining Lemma 4.4, (4.16), and (4.17), we can write

$$Y(p) \equiv F\left(\frac{p-1}{2}\right) \pmod{p^2},$$

where

$$F(n) := \sum_{j=1}^{n} \binom{n+j}{j}^2 \binom{n}{j}^2 (1 + 2jH_{n+j}^{(1)} + 2jH_{n-j}^{(1)} - 4jH_j^{(1)}).$$

By Theorem 7 in [1], $F(n) = 0$ for all positive integers n, proving the second assertion of Proposition 3.1.

Finally, by Proposition 2.1, we see that $\Gamma_p\big(\frac{1}{2}\big)^4/\Gamma_p(1)^4 = 1$. Thus by (3.9), it remains to show that

$$Z(p) = \sum_{j=0}^{(p-1)/2} \frac{\Gamma_p\big(\frac{1}{2}+j\big)^4}{\Gamma_p(1+j)^4} \equiv \sum_{j=0}^{(p-1)/2} \binom{2j}{j}^4 2^{-8j} \pmod{p^3}.$$

In fact, we have equality by the following lemma.

Lemma 4.5. *Let p be an odd prime. Then*

$$\sum_{j=0}^{(p-1)/2} \frac{\Gamma_p\big(\frac{1}{2}+j\big)^4}{\Gamma_p(1+j)^4} = \sum_{j=0}^{(p-1)/2} \binom{2j}{j}^4 2^{-8j}.$$

Proof. Using Proposition 2.1(2) we can write

$$\begin{aligned}\Gamma_p\left(\frac{1}{2}+j\right) &= \frac{\Gamma_p\big(\frac{1}{2}+j\big)}{\Gamma_p\big(\frac{1}{2}+j-1\big)} \frac{\Gamma_p\big(\frac{1}{2}+j-1\big)}{\Gamma_p\big(\frac{1}{2}+j-2\big)} \cdots \frac{\Gamma_p\big(\frac{3}{2}\big)}{\Gamma_p\big(\frac{1}{2}\big)} \Gamma_p\left(\frac{1}{2}\right)\\ &= (-1)^j \frac{2j-1}{2} \cdot \frac{2j-3}{2} \cdots \frac{1}{2} \Gamma_p\left(\frac{1}{2}\right).\end{aligned}$$

Taking fourth powers gives us

$$\Gamma_p\left(\frac{1}{2}+j\right)^4 = 2^{-4j}(2j-1)^4(2j-3)^4 \cdots 3^4.$$

On the other hand, we see that

$$\left(\frac{2j!}{j!}\right)^4 = \left(\frac{2j(2j-1)(2j-2)\cdots 2\cdot 1}{j(j-1)(j-2)\cdots 2\cdot 1}\right)^4 = 2^{4j}(2j-1)^4(2j-3)^4\cdots 3^4.$$

We know that $\Gamma_p(1+j)^4 = (j!)^4$, so

$$\frac{\Gamma_p\big(\frac{1}{2}+j\big)^4}{\Gamma_p(1+j)^4} = \binom{2j}{j}^4 2^{-8j}.$$

This proves our lemma, and so finishes the proof of Proposition 3.1 and Theorem 1. ∎

Acknowledgments. The author would like to thank Scott Ahlgren for his helpful discussions while writing this paper, and the anonymous referee for his insightful comments.

References

[1] S. Ahlgren and K. Ono, *A Gaussian hypergeometric series evaluation and Apéry number congruences*, J. Reine Angew. Math. 518 (2000), 187–212.

[2] —, —, *Modularity of a certain Calabi–Yau threefold*, Monatsh. Math. 129 (2000), 177–190.

[3] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums*, Canad. Math. Soc. Ser. Monographs Adv. Texts, Wiley, New York, 1998.

[4] F. Beukers, *Another congruence for the Apéry numbers*, J. Number Theory 25 (1987), 201–210.

[5] S. Chowla, B. Dwork and R. Evans, *On the mod p^2 determination of $\binom{(p-1)/2}{(p-1)/4}$*, ibid. 24 (1986), 188–196.

[6] B. van Geemen and N. O. Nygaard, *On the geometry and arithmetic of some Siegel modular threefolds*, ibid. 53 (1995), 45–87.

[7] B. H. Gross and N. Koblitz, *Gauss sums and the p-adic Γ-function*, Ann. of Math. (2) 109 (1979), 569–581.

[8] T. Ishikawa, *On Beukers' conjecture*, Kobe J. Math. 6 (1989), 49–51.

[9] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, 2nd ed., Grad. Texts in Math. 58, Springer, New York, 1984.

[10] E. Mortenson, *A supercongruence conjecture of Rodriguez-Villegas for a certain truncated hypergeometric function*, J. Number Theory 99 (2003), 139–147.

[11] —, *Supercongruences between truncated ${}_2F_1$ hypergeometric functions and their Gaussian analogs*, Trans. Amer. Math. Soc. 355 (2003), 987–1007 (electronic).

[12] —, *Supercongruences for truncated ${}_{n+1}F_n$ hypergeometric series with applications to certain weight three newforms*, Proc. Amer. Math. Soc. 133 (2005), 321–330 (electronic).

[13] F. Rodriguez-Villegas, *Hypergeometric families of Calabi–Yau manifolds*, in: Calabi–Yau Varieties and Mirror Symmetry (Toronto, ON, 2001), Fields Inst. Commun. 38, Amer. Math. Soc., Providence, RI, 2003, 223–231.

[14] H. A. Verrill, *Arithmetic of a certain Calabi–Yau threefold*, in: Number Theory (Ottawa, ON, 1996), CRM Proc. Lecture Notes 19, Amer. Math. Soc., Providence, RI, 1999, 333–340.

Department of Mathematics
University of Illinois
Urbana, IL 61801, U.S.A.
E-mail: tkilbour@math.uiuc.edu

Received on 9.3.2005
and in revised form on 31.1.2006 (4955)