A Gaussian hypergeometric series evaluation and Apéry number congruences

Article *in* Journal für die reine und angewandte Mathematik · January 2000

DOI: 10.1515/crll.2000.004

Ken Ono
Emory University

A GAUSSIAN HYPERGEOMETRIC SERIES EVALUATION AND APÉRY NUMBER CONGRUENCES

Scott Ahlgren and Ken Ono

To appear in J. reine ange. Math.

In celebration of B. C. Berndt's sixtieth birthday.

Abstract. If p is prime, then let ϕ_p denote the Legendre symbol modulo p and let ϵ_p be the trivial character modulo p. As usual, let ${}_{n+1}F_n(x)_p := {}_{n+1}F_n\left(\begin{matrix}\phi_p, & \phi_p, & \dots, & \phi_p \\ & \epsilon_p, & \dots, & \epsilon_p\end{matrix} \mid x\right)_p$ be the Gaussian hypergeometric series over $\mathbb{F}_p$. For $n > 2$ the non-trivial values of ${}_{n+1}F_n(x)_p$ have been difficult to obtain. Here we take the first step by obtaining a simple formula for ${}_4F_3(1)_p$. As a corollary we obtain a result describing the distribution of traces of Frobenius for certain families of elliptic curves. We also find that ${}_4F_3(1)_p$ satisfies surprising congruences modulo 32 and 11. We then establish a mod p^2 "supercongruence" between Apéry numbers and the coefficients of a certain eta-product; this relationship was conjectured by Beukers in 1987. Finally, we obtain many new mod p congruences for generalized Apéry numbers.

1. Introduction and Statement of Results

Let p be an odd prime, and let $\mathbb{F}_p$ denote the finite field with p elements. We extend all multiplicative characters χ of $\mathbb{F}_p^\times$ to $\mathbb{F}_p$ by defining $\chi(0) := 0$. If A and B are two characters of $\mathbb{F}_p$, then we define the normalized Jacobi sum $\binom{A}{B}$ by

$$\binom{A}{B} := \frac{B(-1)}{p} J(A, \bar{B}) = \frac{B(-1)}{p} \sum_{x \in \mathbb{F}_p} A(x)\bar{B}(1-x).$$

Let $A_0, A_1, \dots A_n$, and $B_1, B_2, \dots B_n$ be characters of $\mathbb{F}_p$. Following Greene [G], we define the Gaussian hypergeometric series over $\mathbb{F}_p$ by

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

(here the sum runs over all characters χ of $\mathbb{F}_p$). Let ϕ_p and ϵ_p denote the quadratic and trivial characters of $\mathbb{F}_p$, respectively, and define ${}_{n+1}F_n(x)_p$ by

$$(1.1) \qquad {}_{n+1}F_n(x)_p := {}_{n+1}F_n\left(\begin{matrix}\phi_p, & \phi_p, & \dots, & \phi_p \\ & \epsilon_p, & \dots, & \epsilon_p\end{matrix} \mid x\right)_p.$$

The second author is supported by grants from the NSA and NSF, and an Alfred P. Sloan Foundation Research Fellowship.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

Many character sums (in particular, the Jacobsthal sums), may be evaluated in terms of the representations of integers by binary quadratic forms (see, for example, [B-E], [B-E-W], [E], and [G-S], among others). As an example, if p is an odd prime, then we have (see [Ch. 6, B-E-W])

$$p \cdot {}_2F_1(-1)_p = \sum_{x=0}^{p-1} \phi_p(x^3 - x) = \begin{cases} (-1)^{\frac{x+y+1}{2}} \cdot 2x & \text{if } p = x^2 + y^2, \text{ and } x > 0 \text{ is odd,} \\ 0 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

In the first part of this paper we obtain a simple formula for ${}_4F_3(1)_p$. If D is a fundamental discriminant of a quadratic field, then let $\chi_D := \left(\frac{D}{\bullet}\right)$ denote the usual Kronecker character. Our main result is the following evaluation of ${}_4F_3(1)_p$, which is given in terms of representations of $4p$ as a sum of four squares.

Theorem 1. *If p is an odd prime, then*

$${}_4F_3(1)_p = -\frac{1}{p^2} - \frac{1}{p^3} \sum_{\substack{a^2+b^2+c^2+d^2=4p \\ a,b,c,d>0}} \chi_{-4}(ab)ab.$$

The proof of Theorem 1 relies in part on the fact that the Calabi-Yau threefold given by

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

is modular in the sense that the number of its points over $\mathbb{F}_p$ is predicted by the Fourier expansion of a certain weight 4 cusp form. This threefold has been studied by Verrill [V]. Its modularity was proved by van Geemen and Nygaard [vG-N] using the method of Serre and Faltings as first implemented by Livne. In a forthcoming paper [A-O] the present authors provide a direct proof.

Theorem 1 together with a theorem of Deligne will imply

Theorem 2. *If p is an odd prime, then*

$$\left| {}_4F_3(1)_p + \frac{1}{p^2} \right| \leq \frac{2}{p^{3/2}}.$$

Koike [K] and Ono [O] developed the relationship between nontrivial values of ${}_2F_1(x)_p$ and ${}_3F_2(x)_p$ and elliptic curves. If $\lambda \neq 0, 1$ then let ${}_2E_1(\lambda)$ denote the Legendre elliptic curve

$$(1.2) \qquad {}_2E_1(\lambda): \quad y^2 = x(x-1)(x-\lambda),$$

and if $\lambda \neq 0, -1$ then let ${}_3E_2(\lambda)$ denote the elliptic curve

$$(1.3) \qquad {}_3E_2(\lambda): \quad y^2 = (x-1)(x^2+\lambda).$$

Let ${}_2N_1(p;\lambda)$ (respectively ${}_3N_2(p;\lambda)$) denote the number of $\mathbb{F}_p$ points (including the point at infinity) on the reduction of ${}_2E_1(\lambda)$ (respectively ${}_3E_2(\lambda)$) modulo p, and define

$$(1.4) \qquad {}_2a_1(p;\lambda) := p + 1 - {}_2N_1(p;\lambda) \quad \text{and} \quad {}_3a_2(p;\lambda) := p + 1 - {}_3N_2(p;\lambda).$$

As a consequence of Theorem 2, we obtain the following "Mean Square" result for the traces of Frobenius of all the distinct reductions of ${}_2E_1(\lambda)$ and ${}_3E_2(\lambda)$ modulo p.

Corollary 1. *If p is an odd prime, then*

$$\left|\sum_{\lambda=2}^{p-1} \frac{\phi_p(\lambda)_2 a_1(p;\lambda)^2}{p}\right| \leq 2\sqrt{p} + 1 + \frac{1}{p},$$
$$\left|\sum_{\lambda=1}^{p-2} \frac{\phi_p(\lambda^2+\lambda)_3 a_2(p;\lambda)^2}{p}\right| \leq 2\sqrt{p} + 2.$$

We also establish congruences relating the values of ${}_4F_3(1)_p$ to p modulo 32 and 11.

Theorem 3. *If p is an odd prime, then*

$$p^3 {}_4F_3(1)_p \equiv -1 - p - p^3 \pmod{32}.$$

By Theorem 2 we see that ${}_4F_3(1)_p$ tends to zero very quickly as $p \to \infty$. However since $1 + p + p^3$ is odd, Theorem 3 yields the following immediate corollary.

Corollary 2. *If p is an odd prime, then*

$${}_4F_3(1)_p \neq 0.$$

Using recent work of Gordon [Go], we will obtain the following surprising congruence.

Theorem 4. *If p is an odd prime, then*

$$\left(p^3 {}_4F_3(1)_p + p\right)^2 \equiv 0, p^3, 2p^3, \text{ or } 4p^3 \pmod{11}.$$

Moreover, if $\delta(i)$, $1 \leq i \leq 4$, denotes the Dirichlet density of primes p for which

$$\left(p^3 {}_4F_3(1)_p + p\right)^2 \equiv ip^3 \pmod{11},$$

then

$$\delta(i) = \begin{cases} 3/8 & \text{if } i = 0, \\ 1/3 & \text{if } i = 1, \\ 1/4 & \text{if } i = 2, \\ 1/24 & \text{if } i = 4. \end{cases}$$

In the last half of the paper we shall focus on the connection between Gaussian hypergeometric series and Apéry numbers. For positive integers n, define the Apéry number

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

(These numbers were used by Apéry in his famous proof that $\zeta(3)$ is irrational.) Define integers $a(n)$ by

$$\sum_{n=1}^{\infty} a(n) q^n := q \prod_{n=1}^{\infty} (1 - q^{2n})^4 (1 - q^{4n})^4. \tag{1.5}$$

In 1987, Beukers [Beu2] proved that for every odd prime p, we have

$$A\left(\frac{p-1}{2}\right) \equiv a(p) \pmod{p}. \tag{1.6}$$

Beukers went on to conjecture that the congruence (1.6) continues to hold modulo p^2. In 1988, Ishikawa [Ish] observed that by combining two formulae of Beukers [Beu2] and Gessel [Ge], one indeed obtains the conjectured mod p^2 congruence in the case when $p \nmid A(\frac{p-1}{2})$. Unfortunately, there are primes p such that $p \mid A(\frac{p-1}{2})$.

As a result of our ${}_4F_3(1)_p$ evaluation in Theorem 6 below, we are able to prove the conjecture unconditionally.

Theorem 5 (Apéry number supercongruence). *Let p be an odd prime. Then*

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

Finally, we consider congruences for generalized Apéry numbers. Given non-negative integers m and ℓ, the generalized Apéry numbers $A(n;m,\ell)$ and $D(n;m,l,r)$ are defined by

$$\begin{aligned} A(n;m,\ell) &:= \sum_{j=0}^{n} \binom{n+j}{j}^m \binom{n}{j}^\ell, \\ D(n;m,l,r) &:= \sum_{j=0}^{n} \binom{n+j}{j}^m \binom{n}{j}^\ell r^{\ell j}. \end{aligned} \tag{1.7}$$

We shall see in Section 3 that Beukers' congruence (1.6) is equivalent to the congruence

$$A\left(\frac{p-1}{2};2,2\right) \equiv \sum_{\substack{a^2+b^2+c^2+d^2=4p \\ a,b,c,d>0}} \chi_{-4}(ab)ab \pmod{p}. \tag{1.8}$$

In the last section we will exploit the connection between Gaussian hypergeometric series, elliptic curves, and the Dedekind eta function in order to obtain congruences similar to (1.8) for generalized Apéry numbers. As a typical example, we will show that if $p \geq 5$, then

$$D\left(\frac{p-1}{2};0,2,2\right) \equiv \sum_{\substack{a^2+2b^2+3c^2+6d^2=12p \\ a,b,c,d>0}} \chi_{12}(abcd) \pmod{p}.$$

Apart from (1.8), most of the other congruences that have been found for generalized Apéry numbers (see [Beu1, Beu-S, K, O]) have been related to elliptic curves with complex multiplication (see [O]). However, (1.8) is an example of a relationship between generalized Apéry numbers and a modular form without complex multiplication. The main feature of this congruence, and others listed in this paper, is the presence of an exceptional quadratic form.

2. Preliminaries

Here we collect various results which we shall need to prove Theorem 1. Since the prime p will always be clear from context, we will ease notation by referring to ${}_{n+1}F_n(x)_p$, ϕ_p, and ϵ_p as ${}_{n+1}F_n(x)$, ϕ, and ϵ, respectively. Unless otherwise noted, our sums will run over all elements of $\mathbb{F}_p$. In [§3,G], Greene gave the formula

$$ {}_2F_1(y) = \frac{\epsilon(y)\phi(-1)}{p} \sum_x \phi(x)\phi(1-x)\phi(1-xy). \tag{2.1} $$

In the same section Greene showed that if $n \geq 1$, then we have the following inductive relationship:

$$ {}_{n+1}F_n(y) = \frac{\phi(-1)}{p} \sum_x \phi(x)\phi(1-x)\,{}_nF_{n-1}(xy). \tag{2.2} $$

From (2.1) and (2.2), we see that if n is a positive integer, then $p^n\,{}_{n+1}F_n(x) \in \mathbb{Z}$.

We shall frequently make use of the following basic fact.

Lemma 2.1. *Let p be an odd prime, and $a \in \mathbb{F}_p$. Then*

(a)

$$ \sum_x \phi(x^2+ax) = \begin{cases} p-1 & \text{if } a=0, \\ -1 & \text{if } a \neq 0. \end{cases} $$

(b)

$$ \sum_x \phi(x^2+a) = \begin{cases} p-1 & \text{if } a=0, \\ -1 & \text{if } a \neq 0. \end{cases} $$

Proof. Part (a) is clear when $a=0$. If $a \neq 0$, then replacing x by $\frac{a}{2}(x-1)$ and making the change of variables $y = 1-x^2$ shows that

$$ \sum_x \phi(x^2+ax) = \sum_x \phi(x^2-1) = \phi(-1)\sum_y \phi(y)\{\phi(1-y)+1\} = \phi(-1)J(\phi,\phi) = -1, $$

since $J(\phi,\phi) = -\phi(-1)$ (see §6 below).

The change of variables $y = x^2+a$ in (b) shows that

$$ \sum_x \phi(x^2+a) = \sum_y \phi(y)\{\phi(y-a)+1\} = \sum_y \phi(y)\phi(y-a). $$

The conclusion in (b) then follows from (a). □

The next two lemmas will be used in the proof of Theorem 1.

Lemma 2.2. *Let p be an odd prime. Then*

$$ p^3\,{}_4F_3(1) = p^2 \sum_y \phi(y)\,{}_2F_1(y)^2. $$

Proof. Two applications of (2.2) show that

$$p_4F_3(1) = \phi(-1)\sum_{x\neq 0}\phi(x)\phi(1-x)_3F_2(x) = \frac{1}{p}\sum_{x\neq 0}\sum_{y\neq 0}\phi(x)\phi(1-x)\phi(y)\phi(1-y)_2F_1(xy)$$

(we may impose the condition $xy \neq 0$ since $\phi(0) = 0$). Replace y with y/x and x with xy, and use (2.1) to find that

$$\begin{aligned} p_4F_3(1) &= \frac{1}{p}\sum_{x\neq 0}\sum_{y\neq 0}\phi\left(1-\frac{1}{x}\right)\phi(1-xy)\phi(y)_2F_1(y) \\ &= \sum_{y\neq 0}\phi(y)_2F_1(y)\cdot\frac{1}{p}\sum_{x\neq 0}\phi(x)\phi(x-1)\phi(1-xy) = \sum_{y}\phi(y)_2F_1(y)^2. \end{aligned}$$

□

Lemma 2.3. *Let p be an odd prime. Then*

$$p^2\sum_i {}_2F_1(i)^2 = p^2 - 2p - 2.$$

Proof. By (2.1) and Lemma 2.1 we have

$$\begin{aligned} p^2\sum_i {}_2F_1(i)^2 &= \sum_{i\neq 0}\sum_{x\neq 0}\sum_{y\neq 0}\phi(x)\phi(1-x)\phi(y)\phi(1-y)\phi(1-ix)\phi(1-iy) \\ &= -1 + \sum_{i}\sum_{x\neq 0}\sum_{y\neq 0}\phi(x)\phi(1-x)\phi(y)\phi(1-y)\phi(1-ix)\phi(1-iy). \end{aligned}$$

Replacing x by $1/x$ and y by $1/y$ gives

$$\begin{aligned} p^2\sum_i {}_2F_1(i)^2 &= -1 + \sum_{i}\sum_{x\neq 0}\sum_{y\neq 0}\phi(x)\phi(x-1)\phi(y)\phi(y-1)\phi(x-i)\phi(y-i) \\ &= -1 + \sum_{x\neq 0}\sum_{y\neq 0}\phi(x^2-x)\phi(y^2-y)\sum_i\phi(i^2-(x+y)i+xy). \end{aligned}$$

Replacing i by $i+(x+y)/2$ and using Lemma 2.1, the inner sum becomes

$$\sum_i \phi(i^2-(x-y)^2/4) = \begin{cases} p-1 & \text{if } x = y \\ -1 & \text{if } x \neq y. \end{cases}$$

Then using Lemma 2.1 several times yields

$$\begin{aligned} p^2\sum_i {}_2F_1(i)^2 &= -1 - \sum_x \phi(x^2-x)\sum_{y\neq x}\phi(y^2-y) + (p-1)\sum_x\phi(x^2-x)^2 \\ &= -1 - \sum_x\phi(x^2-x)\{-1-\phi(x^2-x)\} + (p-2)(p-1) = p^2-2p-2. \end{aligned}$$

□

3. Proof of Theorem 1

Let the integers $a(n)$ be as defined in (1.5). The following theorem will be the main vehicle for obtaining the results in this paper.

Theorem 6. *If p is an odd prime, then*

$$p^3 {}_4F_3(1) = -a(p) - p.$$

Deduction of Theorem 1 from Theorem 6. It will suffice to prove that

$$a(p) = \sum_{\substack{a^2+b^2+c^2+d^2=4p \\ a,b,c,d>0}} \chi_{-4}(ab)ab.$$

Begin by noticing that

$$q^{\frac{1}{2}} \prod_{n=1}^{\infty} (1-q^{2n})^2(1-q^{4n})^2 = q^{\frac{1}{2}} \prod_{n=1}^{\infty} (1-q^{2n})^3 \prod_{n=1}^{\infty} (1-q^{2n})(1+q^{2n})(1+q^{2n}).$$

Two simple applications of Jacobi's triple product identity yield

$$q^{\frac{1}{2}} \prod_{n=1}^{\infty} (1-q^{2n})^2(1-q^{4n})^2 = q^{\frac{1}{2}} \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} (-1)^m (2m+1) q^{m^2+m+n^2+n}.$$

Making the change of variables $a = 2m+1$, $b = 2n+1$ gives

$$q^{\frac{1}{2}} \prod_{n=1}^{\infty} (1-q^{2n})^2(1-q^{4n})^2 = \sum_{a,b>0,\text{ odd}} (-1)^{\frac{a-1}{2}} a q^{\frac{a^2+b^2}{4}}.$$

Recall that

$$\chi_{-4}(a) = \begin{cases} (-1)^{\frac{a-1}{2}} & \text{if } a \text{ is odd} \\ 0 & \text{if } a \text{ is even.} \end{cases}$$

Therefore,

$$q^{\frac{1}{2}} \prod_{n=1}^{\infty} (1-q^{2n})^2(1-q^{4n})^2 = \sum_{a,b>0,\text{ odd}} \chi_{-4}(a) a q^{\frac{a^2+b^2}{4}}.$$

Squaring both sides, we find that

$$\sum_{n=1}^{\infty} a(n) q^n = \sum_{a,b,c,d>0,\text{ odd}} \chi_{-4}(ab) ab q^{\frac{a^2+b^2+c^2+d^2}{4}}.$$

Therefore,

$$a(p) = \sum_{\substack{a^2+b^2+c^2+d^2=4p \\ a,b,c,d>0,\text{ odd}}} \chi_{-4}(ab)ab.$$

If $a^2+b^2+c^2+d^2 = 4p$ and any one of a, b, c, or d is even, then they are all even, whence $\chi_{-4}(ab) = 0$. This observation completes the deduction. $\square$

We devote the remainder of the section to the proof of Theorem 6. For every odd prime p it is proved in [vG-N] and [A-O] that

$$a(p) = p^3 - 2p^2 - 7 - N(p), \tag{3.1}$$

where $N(p)$ is given by

$$N(p) := \#\left\{(x,y,z,w) \in (\mathbb{F}_p^\times)^4 \mid x + \tfrac{1}{x} + y + \tfrac{1}{y} + z + \tfrac{1}{z} + w + \tfrac{1}{w} = 0\right\}.$$

Lemma 3.1. *If $p \geq 3$ is prime, then $N(p) = F(p) + p^3 - 4p^2 + 6p - 4$, where*

$$F(p) := \sum_i \left(\sum_x \phi(x^2 - 1)\phi((x+i)^2 - 1) \right)^2 .$$

Proof of Lemma 3.1. We have

$$N(p) = \sum_a \sum_b \sum_c \#\{x + \tfrac{1}{x} = a\}\#\{y + \tfrac{1}{y} = b\}\#\{z + \tfrac{1}{z} = c\}\#\{w + \tfrac{1}{w} = -a - b - c\}.$$

Notice that $x + 1/x = a$ precisely when $(x - a/2)^2 = a^2/4 - 1$. Therefore

$$\#\{x + \tfrac{1}{x} = a\} = \phi(a^2/4 - 1) + 1 = \phi(a^2 - 4) + 1.$$

Therefore (after replacing a, b, c with $2a$, $2b$, $2c$), we have

$$N(p) = \sum_a \sum_b \sum_c \{\phi(a^2 - 1) + 1\}\{\phi(b^2 - 1) + 1\}\{\phi(c^2 - 1) + 1\}\{\phi((a + b + c)^2 - 1) + 1\}.$$

Replacing c with $c - b$, and subsequently replacing b with $-b$, we find that

$$N(p) = \sum_c \left(\sum_a \{\phi(a^2 - 1) + 1\}\{\phi((a + c)^2 - 1) + 1\} \right)^2 .$$

Expanding and using Lemma 2.1 yields

$$N(p) = \sum_c \left(\left\{ \sum_a \phi(a^2 - 1)\phi((a + c)^2 - 1) \right\} + p - 2 \right)^2 .$$

Expanding again and using Lemma 2.1 gives

$$N(p) = F(p) + 2(p - 2) + p(p - 2)^2 = F(p) + p^3 - 4p^2 + 6p - 4.$$

□

After Lemma 2.2, Lemma 3.1, and (3.1), the proof of Theorem 6 is reduced to establishing the following

Lemma 3.2. *If $p \geq 3$, then*

$$F(p) = 2p^2 - 5p - 3 + p^2 \sum_y \phi(y)_2F_1(y)^2.$$

The proof of Lemma 3.2 occupies the rest of the section. We may write

$$F(p) = \sum_i f(i)^2,$$

with $f(i) := \sum_x \phi(x^2-1)\phi((x+i)^2-1)$. Factoring and rearranging, we find that

$$\begin{aligned} f(i) &= \sum_x \phi(x^2+ix-1-i)\phi(x^2+ix-1+i) \\ &= \sum_x \phi((x+\tfrac{i}{2})^2-(\tfrac{i}{2}+1)^2)\phi((x+\tfrac{i}{2})^2-(\tfrac{i}{2}-1)^2) \\ &= \sum_x \phi(x^2-(\tfrac{i}{2}+1)^2)\phi(x^2-(\tfrac{i}{2}-1)^2). \end{aligned}$$

Replacing i with $2(i+1)$, we obtain $F(p) = \sum_i g(i)^2$, where

$$g(i) := \sum_x \phi(x^2-i^2)\phi(x^2-(i+2)^2).$$

Making the change of variables $y = x^2 - i^2$ gives

$$g(i) = \sum_y \phi(y)\phi(y-4i-4)\{\phi(y+i^2)+1\}.$$

Define

$$h(i) := \sum_x \phi(x)\phi(x-4i-4)\phi(x+i^2). \tag{3.2}$$

Using Lemma 2.1, we find that

$$g(i) = \begin{cases} h(i)+p-1 & \text{if } i=-1 \\ h(i)-1 & \text{if } i \neq -1. \end{cases}$$

Therefore

$$F(p) = \sum_i g(i)^2 = \sum_i \{h(i)-1\}^2 - \{h(-1)-1\}^2 + \{h(-1)+p-1\}^2.$$

It is easy to find that $h(-1) = -1$; from this we obtain

$$F(p) = (p-2)^2 - 4 + \sum_i \{h(i)-1\}^2 = p^2 - 3p + \sum_i h(i)^2 - 2\sum_i h(i). \tag{3.3}$$

Lemma 3.3. *Let $h(i)$ be defined as in* (3.2). *Then $\sum_i h(i) = 1$.*

Proof of Lemma 3.3. Recall that $h(-1) = -1$. If $i \neq -1$, then we may replace x by $(4i+4)x$ in the definition of $h(i)$ to obtain

$$h(i) = \sum_x \phi(x)\phi(x-1)\phi((4i+4)x+i^2) \quad \text{if} \quad i \neq -1. \tag{3.4}$$

Therefore,

$$\sum_{i\neq -1} h(i) = \sum_{x\neq 0,1} \phi(x^2-x) \sum_{i\neq -1} \phi(i^2+(4i+4)x).$$

Since $x \neq 0, 1$, Lemma 2.1 gives

$$\begin{aligned}\sum_{i \neq -1} \phi(i^2 + (4i+4)x) &= \sum_{i \neq -1} \phi((i+2x)^2 - 4x^2 + 4x) \\ &= -1 - \phi((2x-1)^2 - 4x^2 + 4x) = -1 - \phi(1) = -2.\end{aligned}$$

Therefore, using Lemma 2.1, we have

$$\sum_{i \neq -1} h(i) = -2 \sum_x \phi(x^2 - x) = 2,$$

and Lemma 3.3 follows. $\square$

We return to the proof of Lemma 3.2. Notice that if $i \neq 0, -1$, then we may rewrite (3.4) as

$$h(i) = \phi(-1) \sum_x \phi(x)\phi(1-x)\phi\left(\frac{4i+4}{i^2}x + 1\right) = p\, {}_2F_1\left(\frac{-4i-4}{i^2}\right) \quad (i \neq 0, -1). \tag{3.5}$$

After Lemma 3.3 and (3.5), (3.3) becomes

$$F(p) = p^2 - 3p - 2 + h(0)^2 + h(-1)^2 + \sum_{i \neq 0,-1} h(i)^2 = p^2 - 3p + p^2 \sum_{i \neq 0,-1} {}_2F_1\left(\frac{-4i-4}{i^2}\right)^2.$$

Making the change of variables $i = 2/(j-1)$ gives

$$F(p) = p^2 - 3p + p^2 \sum_{j \neq 1,-1} {}_2F_1(1-j^2)^2 = p^2 - 3p + p^2 \sum_j {}_2F_1(1-j^2)^2.$$

(We may remove the condition $j \neq \pm 1$ since ${}_2F_1(0) = 0$.) Setting $y = 1 - j^2$, we obtain

$$\begin{aligned}F(p) &= p^2 - 3p + p^2 \sum_y {}_2F_1(y)^2\{\phi(1-y) + 1\} \\ &= p^2 - 3p + p^2 \sum_y {}_2F_1(y)^2 + p^2 \sum_y {}_2F_1(y)^2 \phi(1-y).\end{aligned} \tag{3.6}$$

Lemma 2.3 and (3.6) give us

$$F(p) = 2p^2 - 5p - 2 + p^2 \sum_y {}_2F_1(y)^2 \phi(1-y) = 2p^2 - 5p - 2 + p^2 \sum_y {}_2F_1(1-y)^2 \phi(y). \tag{3.7}$$

Greene [Th. 4.4, G] proved that

$${}_2F_1(y) = \phi(-1) {}_2F_1(1-y) \quad \text{ if } y \neq 0, 1.$$

Using this together with the facts that $p^2 {}_2F_1(0)^2 = 0$ and $p^2 {}_2F_1(1)^2 = 1$, we find that

$$p^2 \sum_y {}_2F_1(1-y)^2 \phi(y) = p^2 \sum_{y \neq 0,1} {}_2F_1(y)^2 \phi(y) = p^2 \sum_y {}_2F_1(y)^2 \phi(y) - 1.$$

This together with (3.7) gives Lemma 3.2. So Theorem 6 (and hence Theorem 1) is proved. $\square$

4. Proof of Theorem 2 and Corollary 1

Proof of Theorem 2. By Theorem 6, if p is an odd prime, then

$$p^3{}_4F_3(1) = -a(p) - p,$$

where, as in (1.5),

$$\sum_{n=1}^{\infty} a(n)q^n = q\prod_{n=1}^{\infty}(1-q^{2n})^4(1-q^{4n})^4.$$

If $\eta(z) := q^{1/24}\prod_{n=1}^{\infty}(1-q^n)$ is Dedekind's eta function, where $q := e^{2\pi iz}$, then

$$\eta^4(2z)\eta^4(4z) = \sum_{n=1}^{\infty} a(n)q^n.$$

This eta-product is a weight 4 cusp form with respect to the congruence subgroup $\Gamma_0(8)$. In fact it lies in a 1 dimensional space, and so is a normalized eigenform of the Hecke operators. Therefore by Deligne's theorem [D], we know that if p is prime, then

$$|a(p)| \le 2p^{\frac{3}{2}}.$$

The result now follows immediately. $\square$

Deduction of Corollary 1 from Theorem 2. Recall the definitions of ${}_2E_1$ and ${}_2a_1(p;\lambda)$ given in (1.2), (1.4). Koike [K] proved that if $\lambda \in \mathbb{F}_p$ and $\lambda \neq 0, 1$, then

$$ {}_2F_1(\lambda) = -\frac{\phi(-1)\,{}_2a_1(p;\lambda)}{p}. \tag{4.1}$$

Using this together with Lemma 2.2 and the fact that ${}_2F_1(1) = -\phi(-1)/p$, we obtain

$$p^2{}_4F_3(1) = p\sum_{\lambda}\phi(\lambda)\,{}_2F_1(\lambda)^2 = \frac{1}{p} + \sum_{\lambda\neq 0,1}\frac{\phi(\lambda)\,{}_2a_1(p;\lambda)^2}{p}.$$

The first assertion in Corollary 1 now follows easily from Theorem 2.

We turn to the second assertion. The curve defined in (1.3) is obtained via a change of variables from the curve ${}_3E_2$ defined in [O]. A slight reformulation of Theorem 5 in that work shows that if $\lambda \in \mathbb{F}_p$, $\lambda \neq 0, -1$, then

$$ {}_3F_2\left(\frac{\lambda+1}{\lambda}\right) = \frac{\phi(-\lambda)({}_3a_2(p;\lambda)^2 - p)}{p^2}. \tag{4.2}$$

By (2.2) we have

$$p^2{}_4F_3(1) = \phi(-1)p\sum_{x\neq 0,1}\phi(x)\phi(1-x)\,{}_3F_2(x).$$

Making the change of variables $x = (\lambda+1)/\lambda$ and using (4.2), we find that

$$p^2{}_4F_3(1) = \sum_{\lambda\neq 0,-1}\phi(-\lambda^2-\lambda)\frac{{}_3a_2(p;\lambda)^2}{p} - \sum_{\lambda\neq 0,-1}\phi(-\lambda^2-\lambda).$$

By Lemma 2.1 we have $\sum_{\lambda\neq 0,-1}\phi(-\lambda^2-\lambda) = \pm 1$; the second assertion in Corollary 1 then follows from Theorem 2. $\square$

5. Proof of Theorems 3 and 4

Proof of Theorem 3. By Theorem 6, it suffices to prove that if p is an odd prime, then

$$a(p) \equiv 1 + p^3 \pmod{32}.$$

The usual weight 4 Eisenstein series with respect to the full modular group $SL_2(\mathbb{Z})$ is given by

$$E_4(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n,$$

where $\sigma_3(n) := \sum_{d|n} d^3$. Using standard facts about modular forms it is easy to deduce that

$$\mathcal{E}_4(z) := \sum_{n=0}^{\infty} \sigma_3(2n+1) q^{2n+1}$$

is a weight 4 modular form with respect to the congruence subgroup $\Gamma_0(8)$. It suffices to show that the following congruence holds:

$$\mathcal{E}_4(z) \equiv \sum_{n=1}^{\infty} a(n) q^n \pmod{32}.$$

By a theorem of Sturm [Th.1, Stu] we know that the congruence holds if and only if it holds for the first five terms. After examining these terms, we find that the congruence is indeed true. $\square$

Deduction of Theorem 4. In 1992, the second author studied the properties of the ℓ-adic Galois representations associated to the eta-product $\eta^4(2z)\eta^4(4z) = \sum_{n=1}^{\infty} a(n)q^n$, and conjectured that the residual 11-adic Galois representation into $\mathrm{PGL}_2(\mathbb{F}_{11})$ has image S_4. In particular, this implies that if p is prime, then

$$a^2(p) \equiv 0, p^3, 2p^3 \text{ or } 4p^3 \pmod{11}. \tag{5.1}$$

Further, if $\delta(i)$ denotes the Dirichlet density of primes p for which $a^2(p) \equiv ip^3 \pmod{11}$, then the conjecture implies that

$$\delta(i) = \begin{cases} 3/8 & \text{if } i = 0, \\ 1/3 & \text{if } i = 1, \\ 1/4 & \text{if } i = 2, \\ 1/24 & \text{if } i = 4 \end{cases} \tag{5.2}$$

(these densities are easily computed from the Chebotarev density theorem by counting the number of elements in S_4 of order 1, 2, 3, and 4). If we combine (5.1) and (5.2) with Theorem 6, we immediately obtain the statement in Theorem 4. Therefore Theorem 4 is indeed true, since Gordon [Go] has recently proved the conjecture. $\square$

Remark 1. In his work, Gordon followed the methods of Haberland [Ha], who had previously proved a similar congruence. Namely, if $b(n)$ are integers defined by

$$\sum_{n=1}^{\infty} b(n)q^n := \left(1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n\right)\cdot \eta^{24}(z) = q + 216q^2 - 3348q^3 + 13888q^4 + \cdots,$$

then for every prime $p \neq 59$, we have

$$b^2(p) \equiv 0, p^{15}, 2p^{15} \text{ or } 4p^{15} \pmod{59}.$$

This congruence was conjectured by Serre and Swinnerton-Dyer in the early 1970's.

Remark 2. Here we present some data which illustrates the phenomenon in Theorem 4. Let $\delta(i, N)$ denote the proportion of primes $p \leq N$ for which

$$\left(p^3 {}_4F_3(1)_p + p\right)^2 \equiv ip^3 \pmod{11}.$$

A simple MAPLE calculation yields the following data:

N	$\delta(0,N)$	$\delta(1,N)$	$\delta(2,N)$	$\delta(4,N)$
1000	0.383	0.347	0.246	0.024
2000	0.390	0.325	0.252	0.033
3000	0.370	0.336	0.261	0.033
4000	0.379	0.330	0.260	0.031
5000	0.388	0.325	0.251	0.036
6000	0.376	0.333	0.252	0.038
7000	0.380	0.334	0.247	0.039
8000	0.377	0.337	0.247	0.039
9000	0.381	0.336	0.243	0.040
10000	0.375	0.335	0.249	0.041

6. Preliminaries on Gauss sums and the p-adic gamma function

In this section we develop some background material which we shall need in the next section to prove the supercongruence of Theorem 5. Since the theorem is easily verified for $p = 3$, we shall suppose in the next two sections that

$$p \geq 5.$$

We begin with properties of the p-adic gamma function Γ_p. A nice treatment of the gamma function is given in [Ko]. Here we follow, with minor variations, the exposition given in [C-D-E], which is convenient to our purpose. Let $\mathbb{Z}_p$, $\mathbb{Q}_p$, and $\mathbb{C}_p$ be defined as usual, and normalize the absolute value on $\mathbb{C}_p$ by $|p| = \frac{1}{p}$. The gamma function is defined on $\mathbb{Z}_p$ by

$$\Gamma_p(n) := (-1)^n \prod_{j<n,\, p\nmid j} j, \quad \text{for } n \in \mathbb{N},$$

and then by

$$\Gamma_p(x) = \lim_{n \to x} \Gamma_p(n), \text{ for } x \in \mathbb{Z}_p.$$

In this limit we may choose any sequence of integers n which approaches x p-adically. The following are true for $x \in \mathbb{Z}_p$.

$$\Gamma_p(0) = 1. \tag{6.1}$$

$$\frac{\Gamma_p(x+1)}{\Gamma_p(x)} = \begin{cases} -x & \text{if} \quad |x| = 1 \\ -1 & \text{if} \quad |x| < 1. \end{cases} \tag{6.2}$$

$$|\Gamma_p(x)| = 1. \tag{6.3}$$

$$\Gamma_p(x)^2 \Gamma_p(1-x)^2 = 1. \tag{6.4}$$

We make the important note that

$$n! = (-1)^{n+1} \Gamma_p(n+1), \qquad 0 \leq n \leq p-1. \tag{6.5}$$

It is also known that if x, $y \in \mathbb{Z}_p$, and $n \geq 1$, then

$$x \equiv y \pmod{p^n} \implies \Gamma_p(x) \equiv \Gamma_p(y) \pmod{p^n}. \tag{6.6}$$

Define

$$\rho = p^{-\frac{1}{p} - \frac{1}{p-1}}.$$

Suppose that $x_0 \in \mathbb{Z}_p$. Then for $|z| < \rho$, we have the Taylor expansion

$$\Gamma_p(x_0 + z) = \sum_{n=0}^{\infty} a_n z^n, \quad \text{with } a_n \in \mathbb{Q}_p.$$

We know that

$$|a_n| \rho^n \leq 1, \qquad n = 0, 1, \dots .$$

In particular, we find that $|a_1| \leq \frac{1}{\rho} < p$. Since $a_1 \in \mathbb{Q}_p$ (whence $\mathrm{ord}_p(a_1) \in \mathbb{Z}$), we conclude that

$$|\Gamma'_p(x_0)| = |a_1| \leq 1, \quad \text{ if } x_0 \in \mathbb{Z}_p. \tag{6.7}$$

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

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

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

$$a_n z^{n-1} \equiv 0 \pmod{p^{\beta_n}},$$

where β_n is the least integer such that

$$\beta_n \geq n(1 - \tfrac{1}{p} - \tfrac{1}{p-1}) - 1.$$

If $n \geq 2$ and $p \geq 5$, we have $\beta_n \geq \beta_2 \geq 1$. From this we deduce that for $x_0 \in \mathbb{Z}_p$ and $|z| \leq |p|$, we have

$$\Gamma'_p(x_0 + z) \equiv \Gamma'_p(x_0) \pmod{p}. \tag{6.8}$$

Using the same arguments, it is shown in [Prop. 3.11, C-D-E] that if $x_0 \in \mathbb{Z}_p$, $|z| \leq |p|$, and $p \geq 5$, then

$$\Gamma_p(x_0 + z) \equiv \Gamma_p(x_0) + z\Gamma'_p(x_0) \pmod{p^2}. \tag{6.9}$$

Finally, we will consider the logarithmic derivative $G(x) := \frac{\Gamma'_p(x)}{\Gamma_p(x)}$. By (6.3) and (6.7), we find that $G(x) \in \mathbb{Z}_p$ for $x \in \mathbb{Z}_p$. From (6.2), we obtain

$$G(x+1) - G(x) = \frac{1}{x}, \qquad \text{if } x \in \mathbb{Z}_p, \quad |x| = 1. \tag{6.10}$$

We turn now to Gauss sums. Let $\pi \in \mathbb{C}_p$ be a fixed root of $x^{p-1} + p = 0$, and let ζ_p be the unique p-th root of unity in $\mathbb{C}_p$ such that $\zeta_p \equiv 1 + \pi \pmod{\pi^2}$. Then for a character $\chi : \mathbb{F}_p \mapsto \mathbb{C}_p$, we define the Gauss sum

$$g(\chi) = \sum_{x=0}^{p-1} \chi(x)\zeta_p^x.$$

The following properties of Gauss and Jacobi sums are well-known (by conjugation we mean the automorphism of $\mathbb{C}_p$ which maps each root of unity to its inverse).

(1) $g(\chi)g(\bar{\chi}) = \chi(-1)p$.
(2) If χ_1 and χ_2 are not both trivial, but $\chi_1\chi_2 = \epsilon$, then $J(\chi_1, \chi_2) = -\chi_1(-1)$.
(3) If $\chi_1\chi_2 \neq \epsilon$, then $J(\chi_1, \chi_2) = \dfrac{g(\chi_1)g(\chi_2)}{g(\chi_1\chi_2)}$.

Using the first two properties, we find that

$$g(\phi)^4 = p^2 \quad \text{ and } \quad J(\phi, \phi)^4 = 1. \tag{6.11}$$

Let ω denote the Teichmüller character; ω is a primitive character which is defined uniquely by the property that $\omega(x) \equiv x \pmod{p}$ for $x = 0, \ldots, p-1$. In the current context, the Gross-Koblitz formula [Gr-Ko] states that

$$g(\bar{\omega}^j) = -\pi^j \Gamma_p\left(\frac{j}{p-1}\right), \qquad 0 \leq j \leq p-2. \tag{6.12}$$

7. Proof of Beukers' conjecture

This section contains the proof of Theorem 5. In our first two lemmas, we rewrite each side of the desired congruence in terms of the p-adic gamma function.

Lemma 7.1. *Let the integers $a(n)$ be defined by* (1.5)*. Then for primes $p \geq 5$, we have*

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

Proof. Using properties of Jacobi sums, one finds the identity $\binom{\phi\chi}{\chi}\chi(-1) = \binom{\phi}{\chi}$ for all χ. Therefore, proceeding from the definition (1.1), we obtain

$$(7.1) \qquad {}_4F_3(1) = \frac{p}{p-1} \sum_{\chi} \binom{\phi}{\chi}^4 = \frac{p}{p-1} \sum_{\chi} \binom{\phi}{\bar{\chi}}^4 = \frac{1}{p^3(p-1)} \sum_{\chi} J(\phi,\chi)^4.$$

By (6.11) and the third property above, we see that

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

Let ω be the Teichmüller character; then

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

By the Gross-Koblitz formula, we find that

$$\sum_{\chi} J(\phi,\chi)^4 = 1 + \sum_{j=0}^{\frac{p-3}{2}} \frac{\Gamma_p(\frac{j}{p-1})^4}{\Gamma_p(\frac{j}{p-1}+\frac{1}{2})^4} + p^4 \sum_{j=\frac{p+1}{2}}^{p-2} \frac{\Gamma_p(\frac{j}{p-1})^4}{\Gamma_p(\frac{j}{p-1}-\frac{1}{2})^4}.$$

This together with (7.1) shows that

$$p^3{}_4F_3(1) \equiv \frac{1}{p-1} \left(1 + \sum_{j=0}^{\frac{p-3}{2}} \frac{\Gamma_p(\frac{j}{p-1})^4}{\Gamma_p(\frac{j}{p-1}+\frac{1}{2})^4} \right) \pmod{p^2}.$$

Using this together with Theorem 6, we obtain

$$\begin{aligned} a(p) = -p^3{}_4F_3(1) - p \equiv& \frac{-1}{p-1} \left(1 + \sum_{j=0}^{\frac{p-3}{2}} \frac{\Gamma_p(\frac{j}{p-1})^4}{\Gamma_p(\frac{j}{p-1}+\frac{1}{2})^4} \right) - p \pmod{p^2} \\ \equiv& 1 + (p+1) \sum_{j=0}^{\frac{p-3}{2}} \frac{\Gamma_p(\frac{j}{p-1})^4}{\Gamma_p(\frac{j}{p-1}+\frac{1}{2})^4} \pmod{p^2}. \end{aligned}$$

Now $\frac{j}{p-1} \equiv -j - jp \pmod{p^2}$, so that

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

Replacing j by $\frac{p-1}{2} - j$ in this sum and using (6.6) gives the lemma. $\square$

Lemma 7.2. *Recall the definition of the Apéry number*

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

Then for primes $p \geq 5$, we have

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

Proof. Using (6.5), we obtain

$$A\left(\frac{p-1}{2}\right) = \sum_{j=0}^{\frac{p-1}{2}} \frac{(\frac{p-1}{2}+j)!^2}{j!^4(\frac{p-1}{2}-j)!^2} = \sum_{j=0}^{\frac{p-1}{2}} \frac{\Gamma_p(\frac{1}{2}+j+\frac{p}{2})^2}{\Gamma_p(1+j)^4\Gamma_p(\frac{1}{2}-j+\frac{p}{2})^2}.$$

Then, by (6.4), we find that

$$A\left(\frac{p-1}{2}\right) = \sum_{j=0}^{\frac{p-1}{2}} \frac{\Gamma_p(\frac{1}{2}+j+\frac{p}{2})^2\Gamma_p(\frac{1}{2}+j-\frac{p}{2})^2}{\Gamma_p(1+j)^4}.$$

Notice that (6.9) and (6.7) yield

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

The lemma follows easily. $\square$

We are now in a position to prove the conjecture. Recall that $G(x)$ is the logarithmic derivative of $\Gamma_p(x)$. Using Lemma 7.1 together with (6.9), we compute:

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

Multiplying top and bottom of the jth term by $1-4jpG(1+j)$, and using Lemma 7.2, we find that

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

(In the second step we use the fact, easily deduced from (6.4), that $\Gamma_p(\frac{1}{2})^4 = 1$.) We conclude that the proof of Theorem 5 will be finished after we establish

Lemma 7.3. *If $p \geq 5$ is prime, then*

$$\sum_{j=1}^{\frac{p-1}{2}} \frac{\Gamma_p(\frac{1}{2}+j)^4}{\Gamma_p(1+j)^4} \left(1 + 4j\{G(\tfrac{1}{2}+j) - G(1+j)\}\right) \equiv 0 \pmod{p}.$$

Proof of Lemma 7.3. Arguing as in Lemma 7.2, we find that

$$\frac{\Gamma_p(\frac{1}{2}+j)^4}{\Gamma_p(1+j)^4} \equiv \binom{\frac{p-1}{2}+j}{j}^2 \binom{\frac{p-1}{2}}{j}^2 \pmod{p}. \tag{7.2}$$

For a non-negative integer m, define

$$H_m := 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{m}.$$

By (6.6) and (6.8), we find that

$$G(\tfrac{1}{2}+j) - G(1+j) \equiv G(\tfrac{p+1}{2}+j) - G(1+j) \pmod{p}.$$

Then, using property (6.10) repeatedly on the right side, we find that

$$G(\tfrac{1}{2}+j) - G(1+j) \equiv H_{\frac{p-1}{2}+j} - H_j \pmod{p}. \tag{7.3}$$

By pairing terms from the inside out, we find that

$$H_{\frac{p-1}{2}+j} - H_{\frac{p-1}{2}-j} = \frac{1}{\frac{p-1}{2}-j+1} + \cdots + \frac{1}{\frac{p-1}{2}} + \frac{1}{\frac{p+1}{2}} + \cdots + \frac{1}{\frac{p-1}{2}+j} \equiv 0 \pmod{p}.$$

This together with (7.3) shows that

$$4j\left(G(\tfrac{1}{2}+j) - G(1+j)\right) \equiv 2jH_{\frac{p-1}{2}+j} + 2jH_{\frac{p-1}{2}-j} - 4jH_j \pmod{p}.$$

Combining this with (7.2) we conclude that it will suffice to show that

$$\sum_{j=1}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}+j}{j}^2 \binom{\frac{p-1}{2}}{j}^2 \left(1 + 2jH_{\frac{p-1}{2}+j} + 2jH_{\frac{p-1}{2}-j} - 4jH_j\right) \equiv 0 \pmod{p}.$$

Actually much more is true. The proof of Lemma 7.3, and hence the proof of Theorem 5 is complete, in view of

Theorem 7. *For any positive integer n, define*

$$F(n) = \sum_{j=1}^{n} \binom{n+j}{j}^2 \binom{n}{j}^2 \left(1 + 2jH_{n+j} + 2jH_{n-j} - 4jH_j\right). \tag{7.4}$$

Then

$$F(n) = 0.$$

Proof of Theorem 7. This identity is the subject of [A-E-O-Z]. The summand in (7.4) is the product of a hypergeometric term and a "WZ potential function". By [Th. 9, Z], we are guaranteed that $F(n)$ satisfies a non-trivial linear recurrence relation. Indeed, we find that

$$a_0(n)F(n) + a_1(n)F(n+1) + a_2(n)F(n+2) + a_3(n)F(n+3) = 0, \quad n = 1, 2, 3, \ldots,$$

where the a_i are certain polynomials, and a_3 has no positive integer roots. Since $F(1) = F(2) = F(3) = 0$, we may conclude that $F(n) = 0$ for all n. For details, see [A-E-O-Z]. $\square$

8. Generalized Apéry Number Congruences

Ono [Prop. 5, O] proved for the numbers $D(n; m, \ell, r)$ that

Lemma 8.1. *If $p = 2f + 1$ is prime, and $w = m + \ell$, then*

$$D(f; m, \ell, r) \equiv \left(\frac{p}{p-1}\right)^{w-1} {}_wF_{w-1}((-r)^\ell) \pmod{p}.$$

By classifying all of the curves ${}_2E_1(\lambda)$ and ${}_3E_2(\lambda)$ which have complex multiplication, one obtains closed formulae for ${}_2F_1(x)$ and ${}_3F_2(x)$ for certain special x in terms of the values of Hecke Grössencharacters. Then these formulae imply Apéry number congruences by Lemma 8.1. Apart from (1.8), all of the known Apéry number congruences found in [Beu1, Beu-St, K, O] can be obtained in this way. This analysis is contained in [O]. We will now show that such congruences can be obtained even in the absence of complex multiplication.

For the duration, we will use the notation

$$\begin{aligned}
\sum_{n=1}^{\infty} a_{14}(n)q^n &:= \eta(z)\eta(2z)\eta(7z)\eta(14z),\\
\sum_{n=1}^{\infty} a_{15}(n)q^n &:= \eta(z)\eta(3z)\eta(5z)\eta(15z),\\
\sum_{n=1}^{\infty} a_{20}(n)q^n &:= \eta^2(2z)\eta^2(10z),\\
\sum_{n=1}^{\infty} a_{24}(n)q^n &:= \eta(2z)\eta(4z)\eta(6z)\eta(12z).
\end{aligned} \tag{8.1}$$

By Euler's Pentagonal Number Theorem we see that

$$\eta(24z) = \sum_{n\geq 1} \chi_{12}(n) q^{n^2}.$$

Therefore, for all p, we have

$$\begin{aligned}
a_{14}(p) &= \sum_{\substack{a^2+2b^2+7c^2+14d^2=24p\\ a,b,c,d>0}} \chi_{12}(abcd),\\
a_{15}(p) &= \sum_{\substack{a^2+3b^2+5c^2+15d^2=24p\\ a,b,c,d>0}} \chi_{12}(abcd),\\
a_{20}(p) &= \sum_{\substack{a^2+b^2+5c^2+5d^2=12p\\ a,b,c,d>0}} \chi_{12}(abcd),\\
a_{24}(p) &= \sum_{\substack{a^2+2b^2+3c^2+6d^2=12p\\ a,b,c,d>0}} \chi_{12}(abcd).
\end{aligned}$$

If one prefers, the congruences of Theorems 8 and 9 may be written in terms of these character sums.

Theorem 8. (The ${}_2F_1$ congruences) *Let $p = 2f + 1$ be prime.*

(1) *If $p \neq 2, 3, 5$, then*

$$\left.\begin{array}{l} D(f;0,2,\pm 3/5) \\ D(f;1,1,-9/25) \\ D(f;0,2,\pm 5/3) \\ D(f;1,1,-25/9) \\ D(f,1,1,9/16) \end{array}\right\} \equiv \phi(-1)a_{15}(p) \pmod{p},$$

and

$$\left.\begin{array}{l} D(f;0,2,\pm 5/4) \\ D(f;1,1,-25/16) \\ D(f;0,2,\pm 4/5) \\ D(f;1,1,-16/25) \\ D(f,1,1,16/9) \end{array}\right\} \equiv a_{15}(p) \pmod{p}.$$

(2) *If $p \neq 2, 3$, then*

$$\left.\begin{array}{l} D(f;0,2,\pm 1/2) \\ D(f;1,1,-1/4) \\ D(f;0,2,\pm 2) \\ D(f;1,1,-4) \end{array}\right\} \equiv a_{24}(p) \pmod{p},$$

$$\left.\begin{array}{l} D(f;1,1,3) \\ D(f;1,1,-3/4) \end{array}\right\} \equiv \phi(-1)a_{24}(p) \pmod{p},$$

$$D(f;1,1,-4/3) \equiv \phi(-3)a_{24}(p) \pmod{p},$$

and

$$D(f;1,1,1/3) \equiv \phi(3)a_{24}(p) \pmod{p}.$$

Method of proof. In the interest of space, we shall not provide all of the details of the proof of this or the next theorem. Instead, we will illustrate how these congruences were obtained by proving that

$$D(f;0,2,2) \equiv a_{24}(p) \pmod{p} \quad \text{if } p \neq 2, 3.$$

By Lemma 8.1 and (4.1), it suffices to determine the residue of

$$-p\,{}_2F_1(4) \equiv \phi(-1)\,{}_2a_1(p;4) \pmod{p}.$$

The elliptic curve

$${}_2E_1(4) : y^2 = x^3 - 5x^2 + 4x$$

has conductor 48 and j-invariant 35152/9. It is the -1-quadratic twist of the conductor 24 curve

$$E : y^2 = x^3 + 5x^2 + 4x.$$

By [Th. 2, M-O] it is known that the L-function of E is

$$L(E, s) := \sum_{n=1}^{\infty} \frac{a_{24}(n)}{n^s}.$$

Therefore, if $p \geq 5$ is prime, then we have

$$_2a_1(p,4) = \phi(-1)a_{24}(p),$$

from which

$$D(f;0,2,2) \equiv a_{24}(p) \pmod{p}.$$

□

All of the congruences in Theorem 8 were obtained in this manner. Every elliptic curve E whose L-function is the Mellin transform of an eta-product is listed in [Th. 2, M-O]. Our congruences were discovered by finding every curve of the form $_2E_1(\lambda)$ which is a quadratic twist of such a curve E.

One can carry out the same analysis for the curves $_3E_2(\lambda)$, in this case using Lemma 8.1 and (4.2), in order to obtain the following congruences.

Theorem 9. (The $_3F_2$ congruences) *Let $p = 2f+1$ be prime.*

(1) *If $p \neq 2,7,13$, then*

$$\left.\begin{array}{l} D(f;2,1,-2^9/7^3) \\ D(f;0,3,-2^3/7) \end{array}\right\} \equiv \phi(-7)a_{14}^2(p) \pmod{p}.$$

(2) *If $p \neq 2,3,5,41$, then*

$$D(f;2,1,2^6\cdot 5^2/3^4) \equiv a_{15}^2(p) \pmod{p}.$$

(3) *If $p \neq 2,3,5,7$, then*

$$\left.\begin{array}{l} D(f;2,1,-2^6\cdot 3^2/5^4) \\ D(f;1,2,\pm 2^3\cdot 3/5^2) \end{array}\right\} \equiv a_{15}^2(p) \pmod{p}.$$

(4) *If $p \neq 2,3,5,17$, then*

$$D(f;2,1,3^2\cdot 5^2/2^6) \equiv a_{15}^2(p) \pmod{p}.$$

(5) *If $p \neq 2,5$, then*

$$D(f;2,1,-5/4) \equiv \phi(-1)a_{20}^2(p) \pmod{p}.$$

(6) *If $p \neq 2,3,7$, then*

$$D(f;2,1,48) \equiv a_{24}^2(p) \pmod{p}.$$

(7) *If $p \neq 2,3$, then*

$$D(f;2,1,-3/4) \equiv a_{24}^2(p) \pmod{p}.$$

(8) *If $p \neq 2,3,5$, then*

$$D(f;2,1,16/9) \equiv a_{24}^2(p) \pmod{p}.$$

Acknowledgements

We thank the referee for their insightful suggestions.

References

[A-E-O-Z] S. Ahlgren, S. Ekhad, K. Ono, and D. Zeilberger, *A binomial coefficient identity related to Beukers' conjecture*, Elec. J. Comb. **5** (1998), R10.

[A-O] S. Ahlgren and K. Ono, *The modularity of a certain Calabi-Yau threefold*, to appear.

[B-E] B.C. Berndt and R.J. Evans, *Sums of Gauss, Jacobi, and Jacobsthal*, J. Number Theory **11** (1979), 349-398.

[B-E-W] B.C. Berndt, R.J. Evans, and K.S. Williams, *Gauss and Jacobi sums*, Wiley Publ., New York, 1998.

[Beu1] F. Beukers, *Some congruences for the Apéry numbers*, J. Number Theory **21** (1985), 141-155.

[Beu2] F. Beukers, *Another congruence for the Apéry numbers*, J. Number Theory **25** (1987), 201-210.

[Beu-S] F. Beukers and J. Stienstra, *On the Picard-Fuchs equation and the formal Brauer group of certain $K3$ surfaces and elliptic curves*, Math. Ann. **271** (1985), 269-304.

[C-D-E] S. Chowla, B. Dwork, and R. Evans, *On the mod p^2 determination of $\binom{(p-1)/2}{(p-1)/4}$*, J. Number Theory **24** (1986), 188-196.

[D] P. Deligne, *La conjecture de Weil I*, Publ. Math. I.H.E.S. **43**.

[E] R.J. Evans, *Character sums over finite fields*, Finite fields, coding theory, and advances in communications and computing (Las Vegas 1991), Lect. Notes. Pure Appl. Math., Dekker, New York **141** (1993), 57-73.

[vG-N] B. van Geemen and N. O. Nygaard, *On the geometry and arithmetic of some Siegel modular threefolds*, J. Number Theory **53** (1995), 45-87.

[Ge] I. Gessel, *Some congruences for the Apéry numbers*, J. Number Theory **14** (1982), 362-368.

[Go] B. Gordon, *Private communication*.

[G] J. Greene, *Hypergeometric series over finite fields*, Trans. Amer. Math. Soc. **301, 1** (1987), 77-101.

[G-S] J. Greene and D. Stanton, *A character sum evaluation and Gaussian hypergeometric series*, J. Number Theory **23** (1986), 136-148.

[Gr-Ko] B. Gross and N. Koblitz, *Gauss sums and the p-adic Γ-function*, Annals of Math. **109** (1979), 569-581.

[Ha] K. von Haberland, *Perioden von modulformen einer variabler und gruppencohomologie I, II, III*, Math. Nachr. **112** (1983), 245-282, 283-295, 297-315.

[Ish] T. Ishikawa, *On Beukers' congruence*, Kobe J. Math **6** (1989), 49-52.

[Ko] N. Koblitz, *p-adic analysis: a short course on recent work*, Cambridge Univ. Press, 1980.

[K] M. Koike, *Hypergeometric series over finite fields and Apéry numbers*, Hiroshima Math. J. **22** (1992), 461-467.

[M-O] Y. Martin and K. Ono, *Eta-quotients and elliptic curves*, Proc. Amer. Math. Soc. **125** (1997), 3169-3176.

[O] K. Ono, *Values of Gaussian hypergeometric series*, Trans. Amer. Math. Soc **350** (1998), 1205-1223.

[Stu] J. Sturm, *On the congruence of modular forms*, Springer Lect. Notes **1240** (1984), 275-280.

[V] H. Verrill, *Arithmetic of a certain Calabi-Yau threefold*, Proc. Fifth Meeting of the Can. Numb. Th. Assoc., to appear.

[Z] D. Zeilberger, *Closed form (pun intended!)*, Contemp. Math. **143** (1993), 579-607.

Department of Mathematics, Penn State University, University Park, Pa. 16802
E-mail address: ahlgren@math.psu.edu

Department of Mathematics, Penn State University, University Park, Pa. 16802
E-mail address: ono@math.psu.edu