Available online at www.sciencedirect.com

ScienceDirect

Indagationes Mathematicae 33 (2022) 946–955

indagationes mathematicae

www.elsevier.com/locate/indag

Some supercongruences of arbitrary length[☆]

Frits Beukers[a,*], Eric Delaygue[b]

[a] Utrecht University, Department of Mathematics, P.O. Box 80.010, 3508 TA Utrecht, Netherlands
[b] Univ Lyon, Université Claude Bernard Lyon 1, CNRS UMR 5208, Institut Camille Jordan, F-69622 Villeurbanne, France

Received 16 March 2022; accepted 11 April 2022

Communicated by G. Cornelissen

Abstract

We prove supercongruences modulo p^2 for values of truncated hypergeometric series at some special points. The parameters of the hypergeometric series are d copies of $1/2$ and d copies of 1 for any integer $d \geq 2$. In addition we describe their relation to hypergeometric motives.

Keywords: Super congruence; Hypergeometric series; Zeta function; Unit root

1. Introduction

Fix an integer $d \geq 2$ and consider the hypergeometric series

$$F(z) = \sum_{n=0}^{\infty} \left(\frac{(1/2)_n}{n!} \right)^d z^n,$$

where $(x)_n$ denotes the product $x(x+1)(x+2)\cdots(x+n-1)$. It is known as the Pochhammer symbol. Let p be a fixed odd prime. For every integer $s \geq 0$ we define the truncated series

☆ The authors would like to thank the Matrix Institute and the organizers of the workshop Hypergeometric Motives and Calabi–Yau Differential Equations for the wonderful and stimulating environment in which this research arose. This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 648132.

* Corresponding author.

E-mail addresses: f.beukers@uu.nl (F. Beukers), delaygue@math.univ-lyon1.fr (E. Delaygue).

URLs: http://www.staff.science.uu.nl/~beuke106/ (F. Beukers), http://math.univ-lyon1.fr/~delaygue/ (E. Delaygue).

https://doi.org/10.1016/j.indag.2022.04.002

0019-3577/

$$F_{p^s}(z)=\sum_{n=0}^{p^s-1}\left(\frac{(1/2)_n}{n!}\right)^d z^n.$$

In particular $F_1(z)=1$. Let z_0 be a p-adic unit and suppose that $F_p(z_0)$ is also a p-adic unit. Then, by a result of Dwork [3], we have for all $s\geq 1$ that $F_{p^s}(z_0)$ is a p-adic unit together with the congruence

$$\frac{F_{p^{s+1}}(z_0)}{F_{p^s}(z_0)}\equiv\frac{F_{p^s}(z_0)}{F_{p^{s-1}}(z_0)}(\text{mod } p^s). \tag{1}$$

So the sequence of quotients is a p-adic Cauchy sequence. We define the limit

$$f(z_0)=\lim_{s\to\infty}\frac{F_{p^s}(z_0)}{F_{p^{s-1}}(z_0)}.$$

The number $f(z_0)$ is referred to as the *unit root part* of the Frobenius-action on a suitable p-adic cohomology. We shall make this a bit more explicit in Section 4.

From (1) it follows that $f(z_0)\equiv F_p(z_0)(\text{mod } p)$. But it turns out that for some values of z_0 one has stronger congruences, a remarkable phenomenon called *supercongruences*. In this paper we prove the following theorem,

Theorem 1.1. *Let $\epsilon_p=(-1)^{d(p-1)/2}$ and suppose that $F_p(\epsilon_p)$ is a p-adic unit. Then*

$$F_p(\epsilon_p)\equiv f(\epsilon_p)(\text{mod } p^2).$$

This proves part of the following conjecture we like to propose here.

Conjecture 1.2. *With the notations as above let $\epsilon=\pm 1$ and suppose that $F_p(\epsilon)$ is a p-adic unit. Then $F_p(\epsilon)\equiv f_p(\epsilon)(\text{mod } p^2)$*

It should be remarked that if $p\equiv 3(\text{mod } 4)$ then $F_p(-\epsilon_p)\equiv 0(\text{mod } p)$ by Corollary 2.4. So the only values $F_p(\epsilon)$ which are still conjectural are $F_p(-1)$ with $p\equiv 1(\text{mod } 4)$.

For some choices of d,ϵ we conjecture some stronger congruences.

Conjecture 1.3. *Suppose that $F_p(\epsilon)$ is a p-adic unit. Then we have $F_p(\epsilon)\equiv f_p(\epsilon)(\text{mod } p^3)$ in the following cases: $d=3$ and $\epsilon=\pm 1$, $d=4$ and $\epsilon=1$, $d=5$ and $\epsilon=1$, $d=6$ and $\epsilon=1$.*

Moreover, in the latter case we expect $F_p(1)\equiv f_p(1)(\text{mod } p^5)$.

There are a number of results which go into this direction, although the formulation does not contain the unit root $f_p(\epsilon)$ but an integer number, usually the pth coefficient of an L-series that occurs in number theory. For example, when $d=2$ Mortenson [7] showed that $F_p(1)\equiv\left(\frac{-4}{p}\right)(\text{mod } p^2)$. Presumably we have $f_p(1)=\left(\frac{-4}{p}\right)$. In general we expect that $f_p(\epsilon)$ is a zero of the pth factor of the global L-series associated to the underlying hypergeometric motive. We explain this more in detail in Section 4

In the case $d=3$ several authors (Ishikawa, Van Hamme, Ahlgren) independently proved that

$$F_p(1)\equiv c_p(\text{mod } p^2)$$

where c_p is the pth coefficient of $\eta(4\tau)^6\in S_3(16,\chi(-4))$, see [8, p 322] and the references therein. The notation $S_k(N,\chi)$ stands for the modular cusp forms of weight k with group $\Gamma_0(N)$

and character χ. In particular $\chi(a)$ stands for the Legendre symbol $\left(\frac{a}{\cdot}\right)$. It is a CM form given by $c_p = 2(a^2-b^2)$ where $p = a^2+b^2$ with a odd. For a proof we refer to [8, Thm 4]. Numerical experiment shows that these congruences do not hold modulo p^3. Surprisingly enough, these experiments also suggest that $F_p(1) \equiv f_p(1) (\mathrm{mod}\ p^3)$. Presumably $f_p(1)$ is the unit root of $x^2 - c_p x + p^2$ corresponding to the local Euler factor of the L-series of the modular form.

Kilbourn [5] has shown that when $d = 4$ we have

$$F_p(1) \equiv a_p (\mathrm{mod}\ p^3),$$

where a_p is the coefficient of the modular form $\eta(2\tau)^4\eta(4\tau)^4 = \sum_{n\geq 1} a_n q^n$, $q = e^{2\pi i\tau}$ in $S_4(8, \chi_0)$. By χ_0 we denote the trivial character. Presumably $f_p(1)$ is the p-adic unit root of $x^2 - a_p x + p^3$ corresponding to the local Eulerfactor at p of the L-series of the modular form. We cannot prove this, but if true it implies that $f_p(1) \equiv a_p (\mathrm{mod}\ p^3)$.

Recently Osburn, Straub, Zudilin [9] proved that $F_p(1) \equiv b_p (\mathrm{mod}\ p^3)$, where b_p is the pth coefficient of the unique newform in $S_6(8, \chi_0)$. It is conjectured that this congruence holds modulo p^5 for all odd p. We believe that $f_p(1)$ is the p-adic unit zero of $x^2 - b_p x + p^5$. Similarly as before this would imply that $f_p(1) \equiv b_p (\mathrm{mod}\ p^5)$.

Beside these results we like to record the following conjecture.

Conjecture 1.4. *We make the implicit assumption that $F_p(-1)$ is a p-adic unit.*

When $d = 3$ we expect $F_p(-1) \equiv c_p (\mathrm{mod}\ p^2)$ where c_p is the pth coefficient of $\eta(\tau)^2\eta(2\tau)\eta(4\tau)\eta(8\tau)^2 \in S_3(8, \chi(-8))$. It is a CM-form with coefficients given by $2(2b^2 - a^2)$ where $p = a^2 + 2b^2$ in case $p \equiv 1, 3 (\mathrm{mod}\ 8)$. As conjectured in Conjecture 1.3 we also expect that $F_p(-1) \equiv f_p(-1) (\mathrm{mod}\ p^3)$.

When $d = 5$ we expect $F_p(-1) \equiv d_p (\mathrm{mod}\ p^2)$ where $d_p = \left(\frac{-8}{p}\right)(\delta_p^2 - 2p^2)$ and δ_p is the pth coefficient of the form $g \in S_3(256, \chi(-4))$ whose expansion starts with

$$g(\tau) = q - 2\sqrt{-2}q^3 + 4q^5 + 8\sqrt{-2}q^7 + q^9 + 10\sqrt{-2}q^{11} + 20q^{13} - 8\sqrt{-2}q^{15} \\ - 10q^{17} - 10\sqrt{-2}q^{19} + 32q^{21} - 8\sqrt{-2}q^{23} + 9q^{25} - 20\sqrt{-2}q^{27} + 20q^{29} + \cdots$$

Since $f_p(-1)$ is (presumably) a zero of $x^2 - d_p x + p^4$ we should have $f_p(-1) \equiv d_p (\mathrm{mod}\ p^4)$. However, experiment shows that $F_p(-1) \equiv f_p(-1)$ only holds modulo p^2. We are indebted to Wadim Zudilin and Dave Roberts for the (conjectural) identification of the coefficients d_p.

A natural, and often asked question, is what happens with the values of $F_{p^s}(\epsilon)$ with $\epsilon = \pm 1$ and $s > 1$. Numerical experiment suggests the following generalization of Theorem 1.1 might be true.

Conjecture 1.5. *Let $\epsilon = \pm 1$ and suppose that $F_p(\epsilon)$ is a p-adic unit. Then we have*

$$F_{p^s}(\epsilon) \equiv f_p(\epsilon) F_{p^{s-1}}(\epsilon) (\mathrm{mod}\ p^{2s})$$

for all integers $s \geq 1$.

Besides supercongruences for hypergeometric sums with parameters 1/2 and 1 there exist several other types for other parameter choices. We refer to [6] for a proof of Rodriguez-Villegas's mod p^3 conjecture for the 14 truncated hypergeometric sums of order 4 corresponding to Calabi–Yau varieties.

The key to the proof of Theorem 1.1 is the special symmetry of the hypergeometric differential equation for $F(z)$. It reads $\theta^d F = z(\theta + 1/2)^d F$, where θ is the derivation $z\frac{d}{dz}$. A simple verification shows that if $F(z)$ is any solution of this differential equation then so is

$z^{-1/2}F(1/z)$. The actual proof of Theorem 1.1 is completely elementary, but at the end of the proof we sketch the role of the symmetry in the background.

2. Proofs

We start with a few well-known elementary congruences.

Lemma 2.1. *For any odd prime p and any integers $0 < b \le a$ we have*

$$\binom{ap}{bp} \equiv \binom{a}{b} (\bmod\ p^2).$$

The theorem was proven by Babbage in 1819, [1]. In 1862 Wolstenholme [11] showed that this congruence holds modulo p^3 for all primes $p \ge 5$.

Proof. Observe that

$$\binom{ap}{bp} = \prod_{k=1}^{(a-b)p} \frac{k+bp}{k}.$$

Split the product into factors with $p|k$ (and write $k = lp$) and factors where k is not divisible by p. We get

$$\binom{ap}{bp} = \prod_{l=1}^{a-b} \frac{l+b}{l} \prod_{\substack{k=1\\(k,p)=1}}^{(a-b)p} \left(1 + \frac{bp}{k}\right),$$

where the second product is restricted to $k \not\equiv 0 (\bmod\ p)$. The first factor equals $\binom{a}{b}$, the second is modulo p^2 equal to

$$1 + \sum_{\substack{k=1\\(k,p)=1}}^{(a-b)p} \frac{bp}{k}.$$

The well-known fact that $\sum_{k=1}^{p-1} 1/k \equiv 0 (\bmod\ p)$ implies that the second product is $1 (\bmod\ p^2)$. This proves our assertion. $\square$

Lemma 2.2. *Let $\gamma = (4^{p-1} - 1)/p$. Then*

$$\sum_{j=1}^{p-1} \frac{(-1)^{j-1}}{j} \equiv \gamma (\bmod\ p).$$

This lemma occurs in the work of Eisenstein [4].

Proof. First notice that

$$\frac{4^{p-1}-1}{p} = \frac{1}{4p}(4^p - 4) = \frac{2^p-2}{p} \frac{2^p+2}{4}.$$

By Fermat the last factor is $1 (\bmod\ p)$ and we get that

$$\frac{4^{p-1}-1}{p} \equiv \frac{2^p-2}{p} (\bmod\ p).$$

We compute the latter modulo p.

$$\frac{1}{p}(2^p-2)=\frac{1}{p}\sum_{k=1}^{p-1}\binom{p}{k}=\sum_{k=1}^{p-1}\frac{1}{k}\binom{p-1}{k-1}.$$

The number $\binom{p-1}{k-1}$ is the coefficient of x^{k-1} in

$$(1+x)^{p-1}\equiv\frac{x^p+1}{x+1}\equiv 1-x+x^2-x^3+\cdots+x^{p-1}(\mathrm{mod}\ p).$$

Hence $\binom{p-1}{k-1}\equiv(-1)^{k-1}(\mathrm{mod}\ p)$ and thus our congruence follows. □

Lemma 2.3. *Define $\alpha_r=\frac{(1/2)_r}{r!}$. Then for any odd prime p and any integer $0\le r<p/2$ we have*

$$\alpha_{\frac{p-1}{2}-r}\equiv(-1)^{\frac{p-1}{2}}\alpha_r(\mathrm{mod}\ p).$$

Proof. Notice that

$$\alpha_r\equiv\frac{(1/2)_r}{r!}\equiv\frac{(1/2-p/2)_r}{r!}\equiv(-1)^r\binom{(p-1)/2}{r}(\mathrm{mod}\ p).$$

The symmetry is now immediate from the last expression. □

A direct corollary is the following.

Corollary 2.4. *Suppose $p\equiv 3(\mathrm{mod}\ 4)$. Then $F_p(-\epsilon_p)\equiv 0(\mathrm{mod}\ p)$.*

Proof. Notice that

$$\begin{aligned}F_p(-\epsilon_p)&=\sum_{r=0}^{(p-1)/2}\alpha_r^d(-\epsilon_p)^r\\&\equiv(-1)^{d(p-1)/2}\sum_{r=0}^{(p-1)/2}\alpha^d_{\frac{p-1}{2}-r}(-\epsilon_p)^r(\mathrm{mod}\ p)\\&\equiv(-1)^{d(p-1)/2}(-\epsilon_p)^{\frac{p-1}{2}}\sum_{r=0}^{(p-1)/2}\alpha_r^d(-\epsilon_p)^r(\mathrm{mod}\ p)\\&\equiv -F_p(-\epsilon_p)(\mathrm{mod}\ p),\end{aligned}$$

which implies our assertion. □

Lemma 2.5. *Let p be an odd prime and r,r',t integers ≥ 0 with $r=pr'+t$ and $t<p$. Let α_r be as in the previous lemma and $\gamma=(4^{p-1}-1)/p$. If $p/2<t$, then p divides α_r and if $t<p/2$ we have*

$$\alpha_r\equiv\alpha_{r'}\alpha_t\left(1-\gamma pr'+2pr'\sum_{j=1}^{2t}\frac{(-1)^{j-1}}{j}\right)(\mathrm{mod}\ p^2).$$

Modulo p the congruence reads $\alpha_r\equiv\alpha_{r'}\alpha_t(\mathrm{mod}\ p)$. This is known as the Lucas-property for α_r.

Proof. Instead of α_r we start with $\binom{2r}{r}$. Notice that

$$\binom{2r}{r} = \binom{2pr'}{pr'} \frac{\prod_{k=1}^{2t}(k+2pr')}{\prod_{k=1}^{t}(k+pr')^2}.$$

Note that if $t > p/2$ the product in the numerator contains the factor $p+2pr'$ and is therefore divisible by p. Suppose from now on that $t < p/2$.

Consider the equation modulo p^2. We apply Lemma 2.1 to the binomial coefficient and get $\binom{2r'}{r'}$. The product over k becomes $\binom{2t}{t}$ times

$$1 + 2pr'\left(\sum_{k=1}^{2t}\frac{1}{k} - \sum_{k=1}^{t}\frac{1}{k}\right) (\mathrm{mod}\ p^2).$$

Notice also that

$$\sum_{k=1}^{2t}\frac{1}{k} - \sum_{k=1}^{t}\frac{1}{k} = \sum_{k=1}^{2t}\frac{(-1)^{k-1}}{k}.$$

Finally use the relation $\binom{2r}{r} = 4^r\alpha_r$. Putting everything together we find that

$$\alpha_r \equiv \alpha_{r'}\alpha_t 4^{r'(1-p)}\left(1 + 2pr'\sum_{k=1}^{2t}\frac{(-1)^{k-1}}{k}\right) (\mathrm{mod}\ p^2).$$

Using $4^{r'(1-p)} \equiv 1 - pr'\gamma (\mathrm{mod}\ p)$ yields our assertion. □

Proof of Theorem 1.1.

In view of congruences (1) it suffices to prove that $F_{p^s}(\epsilon_p) \equiv F_p(\epsilon_p)F_{p^{s-1}}(\epsilon_p) (\mathrm{mod}\ p^2)$ for $s = 2$, but we will do it for all $s \geq 2$. Use the notation $\alpha_r = \frac{(1/2)_r}{r!}$ and Lemma 2.5 to find

$$F_{p^s}(z) = \sum_{r'=0}^{p^{s-1}-1}\sum_{t=0}^{(p-1)/2}(\alpha_{r'}\alpha_t)^d z^{pr'+t}\left(1 - \gamma dpr' + 2dpr'\sum_{k=1}^{2t}\frac{(-1)^{k-1}}{k}\right) (\mathrm{mod}\ p^2).$$

The terms with $t > p/2$ do not occur since $\alpha_r^d \equiv 0 (\mathrm{mod}\ p^2)$ whenever $t > p/2$. This gives

$$F_{p^s}(z) \equiv F_p(z)F_{p^{s-1}}(z^p) + pd\left(G_p(z) - \gamma F_p(z)\right)\sum_{r'=0}^{p^{s-1}-1} r' z^{pr'}\alpha_{r'}^d (\mathrm{mod}\ p^2)$$

where

$$G_p(z) = 2\sum_{t=0}^{(p-1)/2}\left(\sum_{k=1}^{2t}\frac{(-1)^{k-1}}{k}\right)\alpha_t^d z^t.$$

In order to arrive at our result we set $z = \epsilon_p$ and show that $G_p(\epsilon_p) \equiv \gamma F_p(\epsilon_p) (\mathrm{mod}\ p)$. Consider $G_p(\epsilon_p) = 2\Sigma = \Sigma + \Sigma$ as a sum of two (equal) sums over t. In one of these we replace t by $(p-1)/2 - t$ and obtain

$$\sum_{t=0}^{(p-1)/2}\left(\sum_{k=1}^{p-1-2t}\frac{(-1)^{k-1}}{k}\right)\alpha_{(p-1)/2-t}^d \epsilon_p^{(p-1)/2-t}.$$

Apply Lemma 2.3 and replace k in the inner summation by $p-k$. We get

$$\sum_{t=0}^{(p-1)/2}\left(\sum_{k=2t+1}^{p-1}\frac{(-1)^{-p+k-1}}{p-k}\right)\alpha_t^d\epsilon_p^t \pmod{p}.$$

This equals

$$\sum_{t=0}^{(p-1)/2}\left(\sum_{k=2t+1}^{p-1}\frac{(-1)^{k-1}}{k}\right)\alpha_t^d\epsilon_p^t \pmod{p}$$

Thus we obtain after addition of Σ,

$$G_p(\epsilon_p)\equiv\sum_{t=0}^{(p-1)/2}\left(\sum_{k=1}^{p-1}\frac{(-1)^{k-1}}{k}\right)\alpha_t^d\epsilon_p^t\equiv\left(\sum_{k=1}^{p-1}\frac{(-1)^{k-1}}{k}\right)F_p(\epsilon_p) \pmod{p^2}.$$

Application of Lemma 2.2 yields the desired result. □

3. The underlying mechanism

The proof of our main result uses a symmetry of the polynomials $F_p(z), G_p(z)$ modulo p. We show here how this is forced by the symmetry of the hypergeometric equation. One easily sees that $F_p(z) \pmod{p}$ is the unique polynomial of degree $< p/2$ which satisfies our hypergeometric differential equation modulo p and which has constant term 1. Furthermore, $F_p(z)\log z + G_p(z)$ is another solution modulo p. By the symmetry of our equation $z^{(p-1)/2}F_p(1/z)$ is also a polynomial solution modulo p. Hence, by uniqueness of F_p, $z^{(p-1)/2}F_p(1/z)\equiv\lambda F_p(z) \pmod{p}$ for some λ. To determine λ we set $z=\epsilon_p$. Then $\epsilon_p F(\epsilon_p)=\lambda F(\epsilon_p)$. Since $F(\epsilon_p)$ is a p-adic unit by assumption we conclude that $\lambda=\epsilon_p$. Hence $F_p(z)$ is a reciprocal or anti-reciprocal polynomial. We observe that $z^{(p-1)/2}F_p(1/z)\log(1/z)+z^{(p-1)/2}G_p(1/z)$ is also a mod p solution. Multiply by ϵ_p and add $F_p(z)\log z+G_p(z)$. We find the new solution $G_p(z)+\epsilon_p z^{(p-1)/2}G_p(1/z)$ which is a polynomial solution. Hence it equals $\mu F_p(z)$ for some μ. To find the value of μ we set $z=0$. The constant term of $G_p(z)$ is 0 and the constant term of $\epsilon_p z^{(p-1)/2}G_p(1/z)$ is the leading term of $\epsilon_p G_p(z)$, which is $2\sum_{j=1}^{p-1}\frac{(-1)^{j-1}}{j}$, hence 2γ by Lemma 2.2. Using $F_p(0)=1$ we conclude that $\mu=2\gamma$. Now set $z=\epsilon_p$ in

$$\epsilon_p z^{(p-1)/2}G_p(1/z)+G_p(z)\equiv 2\gamma F_p(z) \pmod{p}$$

and we obtain that $G_p(\epsilon_p)=\gamma F_p(\epsilon_p)$, the key step in the proof of our theorem.

4. Hypergeometric motives

In this section we explain the nature of the unit root $f_p(z_0)$ via finite hypergeometric sums and their ζ-functions. For any $q=p^k$ we consider a generator ω of the multiplicative characters on $\mathbb{F}_q^\times$. Then we define the Gauss-sum

$$g_q(\omega^k)=\sum_{x\in\mathbb{F}_q^\times}\omega(x)^k\zeta_p^{\mathrm{Tr}(x)},$$

where $\mathrm{Tr}:\mathbb{F}_q\to\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$ is the trace map and ζ_p is a primitive pth root of unity. Let ϕ be the unique character of order 2. Let $t\in\mathbb{F}_q^\times$ and define

$$H_q(t)=\frac{(-1)^d}{1-q}\sum_{m=0}^{q-2}\left(\frac{g_q(\phi\omega^m)g_q(\omega^{-m})}{g_q(\phi)}\right)^d\omega((-1)^d t)^m.$$

It turns out that the values are rational integers which are independent of the choice of ω and ζ_p. Such functions were introduced by John Greene and independently Nick Katz by the end of the 1980s. According to Katz these sums are traces of the Frobenius operator on l-adic cohomology associated to the hypergeometric differential equation. More concretely, hypergeometric sums show up in point counting results on algebraic varieties over finite fields. The relevant example for us is the following.

Theorem 4.1. *Let q be an odd prime power, $t \in \mathbb{F}_q^\times$ and $d \geq 2$ an integer. Then the number of points with coordinates in $\mathbb{F}_q^\times$ on the hypersurface*

$$X_t : \prod_{i=1}^{d}(x_i + 2 + x_i^{-1}) = 4^d t^{-1}$$

is given by

$$\frac{(q-2)^d - (-1)^d}{q-1} - (-1)^d H_q(t).$$

Proof. This is a consequence of Theorem [2, Thm 6.1]. Since our hypergeometric parameters are just $1/2$ and 1 we are in a special situation where the parameters a_i from [2, Thm 6.1] read $(2, \dots, 2, -1, \dots, -1)$ with d repetitions of 2 and $2d$ repetitions of -1. The corresponding variety is given by the intersection of the following varieties in $(\mathbb{P}^2)^d$,

$$u_1 + v_1 + w_1 = u_2 + v_2 + w_2 = \cdots = u_d + v_d + w_d = 0, \quad \lambda \prod_{i=1}^{d} u_i^2 = \prod_{i=1}^{d} v_i w_i.$$

Elimination of the u_i gives us $\lambda \prod_{i=1}^{d}(v_i + w_i)^2 = \prod_{i=1}^{d} v_i w_i$. Then set $x_i = v_i/w_i$ and $\lambda = t/4^d$ to get the equation of our assertion. Theorem [2, Thm 6.1] gives the point count with invertible coordinates in $\mathbb{F}_q$ as

$$\frac{(q-2)^d}{q-1} + \frac{1}{q^d(q-1)} \sum_{m=1}^{q-2} g_q(\omega^{2m})^d g_q(\omega^{-m})^{2d} \omega(\lambda)^m.$$

Use the Hasse–Davenport relation $g_q(2\,m) = \omega(4)^m g_q(\omega^m) g_q(\phi\omega^m)/g_q(\phi)$ and $g_q(m)g_q(-m) = (-1)^m q$ to get

$$\begin{aligned} &\frac{(q-2)^d}{q-1} + \frac{1}{q-1} \sum_{m=1}^{q-2} \left(\frac{g_q(\phi\omega^m) g_q(\omega^{-m})}{g_q(\phi)} \right)^d \omega((-4)^d \lambda)^m \\ &= \frac{(q-2)^d - (-1)^d}{q-1} - (-1)^d H_q(4^d \lambda) \end{aligned}$$

We find our desired point count after replacing λ by $t/4^d$. $\square$

We now compute ζ-function associated to the values of $H_q(t)$ (with $t \in \mathbb{F}_p^\times$) in the usual way,

$$Z_p(t, T) = \exp\left(\frac{H_{p^s}(t)}{s} T^s \right),$$

which turns out to be a polynomial in $\mathbb{Z}[T]$ of degree d when $t \neq 1$. When $t = 1$ and d odd the degree is $d-1$, when $t = 1$ and d even $Z_p(1, T)$ is a polynomial of degree $d-2$ divided by a factor $1 - p^{-1+d/2}T$. We shall simply take the $d-2$-degree polynomial for $Z_p(1,T)$ in this case.

Here we are not able to prove all this, but we simply mention some folklore results and conjectures which make up a large body of a project on hypergeometric motives by F.Rodriguez-Villegas, D. Roberts and M. Watkins. The latter has implemented the computations in Magma. This is now an impressive library to compute the polynomials $Z_p(T)$, and also to manipulate the global L-series that contain the $Z_p(p^{-s})$ as local Euler factors. In addition K. Kedlaya has recently announced a Sage-implementation (largely a port of the Magma-implementation) which also calculates the $Z_p(T)$ for us.

We use some of these calculations to illustrate the background to the supercongruences and the origin of the unit-root $f_p(z_0)$. The polynomial $Z_p(t,T)$ can be factored as $\prod_i(1-\mu_i T)$ where the μ_i are algebraic and all have the same absolute value $p^{(d-1)/2}$ according to the Weil-conjectures. The exponent $d-1$ is called the weight of the ζ-factor $Z_p(t,T)$. By abuse of language we shall call the μ_i the zeros of $Z_p(t,T)$. The idea is now that if $f_p(z_0)$ is a p-adic unit, the polynomial $Z_p(z_0,T)$ has a unique p-adic zero which is a unit, namely $f_p(z_0)$. Here are some examples.

When $d=4$ and $z_0=1$ we get $Z_p(1,T) = 1 - a_pT + p^3T^2$ where a_p is the pth coefficient of $\eta(2\tau)^4\eta(4\tau)^4$. It is clear that when this polynomial has a unit root $f_p(1)$, the Newton polygon has p-adic slopes 0,3. Hence $f_p(1) \equiv a_p(\mathrm{mod}\ p^3)$. The missing slopes 1, 2 may account for the occurrence of a supercongruence mod p^3.

When $d=6$ and $z_0=1$ we get $Z_p(1,T) = (1 - pa_pT + p^5T^2)(1 - b_pT + p^5T^2)$, where a_p is as above and b_p the pth coefficients of the newform in $S_6(8,\chi_0)$. The Newton slopes of the first one are 1,4 (if a_p is a unit) and 0,5 for the second (if b_p is a unit). This shows that $f_p(1) \equiv b_p(\mathrm{mod}\ p^5)$ and one might also consider this as an explanation for the conjectural supercongruence modulo p^5.

In general, when d is even and $z_0=1$, we expect a factorization $Z_p(1,T) = U_p(T)V_p(T)$ into two factors in $\mathbb{Z}[T]$. The degrees of U_p, V_p are $-1+d/2, -1+d/2$ when $d = 2(\mathrm{mod}\ 4)$ and $-2+d/2, d/2$ if $d \equiv 0(\mathrm{mod}\ 4)$. The factor U_p has one Newton slope 1 and the others higher. The factor V_p, when $f_p(1)$ is a unit, has Newton slopes 0,2 and higher. So, in a way the factorization of $Z_p(1,T)$ separates the slope 1 from the slopes $0, 2, \ldots$. Naturally $f_p(1)$ is the unit root zero of V_p. The separation of the slopes may be seen as an explanation of the supercongruences from Theorem 1.1. Speculations of this type were first made by Dave Roberts and Fernando Rodriguez-Villegas in their preprint [10]. Instead of speaking about Newton slopes they consider Hodge levels in the cohomology of a hypergeometric motive.

Finally we record a few factorizations of $Z_p(-1,T)$ when d is odd. This is a case where factorizations are abundant.

When $d=3$ we get

$$Z_p(-1,T) = (1-pT)(1 - c_pT + \chi(-8)p^2T^2).$$

Here c_p is the pth coefficient of the modular form $\eta(\tau)^2\eta(2\tau)\eta(4\tau)\eta(8\tau)^2$ and is related to the case $d=3$ in Conjecture 1.4.

When $d=5$ we get

$$Z(-1,T) = (1-\gamma_p p^2T)(1 - pc_pT + p^4T^2)(1 - d_pT + p^4T^2),$$

where d_p is the coefficient defined in Conjecture 1.4 and c_p the pth coefficient of $\eta(4\tau)^6$. The coefficient γ_p is -1 if $p \equiv 5(\mathrm{mod}\ 8)$ and 1 otherwise.

When $d = 7$ we get

$$Z_p(-1, T) = (1 - p^3 T)(1 - pa_p T + p^6 T^2)Q_4(T),$$

where Q_4 is a factor of degree 4. Here $a_p = \left(\frac{-4}{p}\right)(\phi_p^2 - 2p^2)$ where ϕ_p is the pth coefficient of the form in $S_3(32, \chi(-4))$ that begins with

$$q+4iq^3+2q^5-8iq^7-7q^9-4iq^{11}-14q^{13}+8iq^{15}+18q^{17}-12iq^{19}+32q^{21}+40iq^{23}+\cdots$$

Moreover, when $p \equiv 3, 5 (\text{mod } 8)$ the polynomial Q_4 factors into $1 - p^6 T^2$ times a quadratic factor $1 - \gamma_p T + p^6 T^2$. However, this does not give us anything stronger than mod p^2 congruences. We are indebted to Dave Roberts for the identification of the modular form.

References

[1] C. Babbage, Demonstration of a theorem relating to prime numbers, Edinburgh Philos. J. 1 (1819) 46–49.
[2] F. Beukers, H. Cohen, A. Mellit, Finite hypergeometric functions, Pure Appl. Math. Quart. 11 (2015) 559–589.
[3] B. Dwork, On p-adic differential equations IV generalized hypergeometric functions as p-adic analytic functions in one variable, annales scientifiques de L'É.N.S. 4º série, Tome 6 (3) (1973) 295–316.
[4] G. Eisenstein, Neue.Gattung. zahlentheoret, Funktionen, die v. 2 elementen abhangen und durch gewisse lineare funktional-gleichungen definiert werden, in: Bericht Über Die Bekanntmachung Zur Geeigneten Verhandlungen Der KÖnigl, Preuß. Akademie der Wissenschaften zu Berlin, 1850, pp. 36–42.
[5] T. Kilbourn, An extension of the Apéry suprecongruences, Acta Arith. 123 (2006) 335–348.
[6] L. Long, F.-T. Tu, N. Yui, W. Zudilin, Supercongruences for rigid hypergeometric calabi–yau threefolds, Adv. in Math 393 (2021) 49 pages, https://doi.org/10.1016/j.aim.2021.108058.
[7] E.T. Mortenson, Supercongruences between truncated ${}_2F_1$ hypergeometric functions and their Gaussian analogues, Trans. Amer. Math. Soc. 355 (2002) 987–1007.
[8] E.T. Mortenson, Supercongruences for truncated ${}_{n+1}F_n$ hypergeometric series with applications to certain weight three forms, Proc. AMS 133 (2005) 321–330.
[9] R. Osburn, A. Straub, W. Zudilin, A modular supercongruence for ${}_6F_5$: an Apéry-like story, Ann. Inst. Fourier 68 (2018) 1987–2004.
[10] D. Roberts, F. Rodriguez-Villegas, Hypergeometric supercongruences, Matrix Institute Annals (2017) 435–439.
[11] J. Wolstenholme, On certain properties of prime numbers, Quart. J. Pure Appl. Math. 5 (1862) 35–39.