SOME SUPERCONGRUENCES OF ARBITRARY LENGTH

FRITS BEUKERS AND ERIC DELAYGUE

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 $d \geq 2$.

1. Introduction

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

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

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

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

In particular $F_0(z) = 1$. Let $z_0$ be a $p$-adic unit and suppose that $F_1(z_0)$ is also a $p$-adic unit. Then, by a result of Dwork we have for all $s \geq 1$ that $F_s(z_0)$ is a $p$-adic unit together with the congruence

$$\frac{F_{s+1}(z_0)}{F_s(z_0)} \equiv \frac{F_s(z_0)}{F_{s-1}(z_0)} \pmod{p^s}.$$

(1)

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

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

The number $f(z_0)$ is referred to as the unit root part of the Frobenius-action on a suitable $p$-adic cohomology (we do not go into the details). From (1) it follows that $f(z_0) \equiv F_1(z_0) \pmod{p}$. 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 $F_1(\epsilon_p)$ is a $p$-adic unit. Then

$$F_1(\epsilon_p) \equiv f(\epsilon_p) \pmod{p^2}.$$
Supercongruences have been the subject of several recent publications, see for example [8] and [7]. In [7] the mod $p^3$ congruences for 14 truncated hypergeometric sums of order 4 (Villegas’s list) are proven. One of the results is a mod $p^3$ congruence for our case $d = 4$. In [8] the authors prove a mod $p^3$ result for the case $d = 6$. However, the right hand sides of these congruences are coefficients of certain modular forms. We think that they coincide with the unit root parts that we consider in this paper, but do not have a proof for this. It is conjectured that in the case $d = 6$ we have congruences modulo $p^5$. Numerical experiments suggest that for $d > 6$ one cannot expect anything better than mod $p^2$ congruences.

The congruences in the present paper concern supercongruences for truncated hypergeometric sums with parameters $1/2, 1$ of any order $d \geq 2$. One might wonder if such results hold for more general parameter sets. At the moment this is not clear. For example in the case of parameter sets $(1/3, 1/3, 1/3, 2/3, 2/3, 2/3)$ and $(1, 1, 1, 1, 1)$ we did not observe any supercongruence.

The key to the results in the present paper is the special symmetry of the hypergeometric differential equation for $F(z)$. It reads $\theta^d F = z(\theta + 1/2)^d F$, where $\theta$ 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 $z^{-1/2}F(1/z)$. This gives a symmetry of the underlying hypergeometric motive. At the end of this paper we briefly indicate its role in the background of the proof of our Theorem 1.1.

2. PROOFS

Lemma 2.1 (Babbage, 1819). For any odd prime $p$ and any integers $0 < b \leq a$ we have

\[
\binom{ap}{bp} \equiv \left(\frac{a}{b}\right) (\mod p^2).
\]

The theorem was proven by Babbage in 1819, [1]. In 1862 Wolstenholme [9] showed that this congruence holds modulo $p^3$ for all primes $p \geq 5$.

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

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

where the second product is restricted to $k \neq 0(\mod p)$. The first factor equals $\binom{a}{b}$, the second is modulo $p^2$ equal to

\[
1 + \sum_{k=1, (k,p)=1}^{p-1} \frac{bp}{k}.
\]

The well-known fact that $\sum_{k=1}^{p-1} 1/k \equiv 0(\mod p)$ implies that the second product is $1(\mod p^2)$. This proves our assertion. □
Lemma 2.2. Let $\gamma = (4^p - 1)/p$. Then

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

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

Proof. First notice that

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

By Fermat the last factor is $1 \pmod{p}$ and we get that

$$\frac{4^p - 1}{p} \equiv \frac{2p - 2}{p} \pmod{p}.$$

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

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

Hence $\binom{p-1}{k-1} \equiv (-1)^{k-1} \pmod{p}$ and thus our congruence follows. \[\square\]

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

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

Proof. Notice that

$$\alpha_r = \left(\frac{1}{2}\right)_r \equiv \frac{(1/2 - p/2)_r}{r!} \equiv (-1)^r \left(\binom{p-1}{r}/r\right) \pmod{p}.$$

The symmetry is now immediate from the last expression. \[\square\]

Lemma 2.4. Let $p$ be an odd prime and $r, r', t$ integers $\geq 0$ with $r = pr' + t$ and $t < p$. Let $\alpha_r$ be as in the previous lemma and $\gamma = (4^p - 1)/p$. If $p/2 < t$, then $p$ divides $\alpha_r$ and if $t < p/2$ we have

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

Modulo $p$ the congruence reads $\alpha_r \equiv \alpha_{r', \alpha_t} \pmod{p}$. This is known as the Lucas-property for $\alpha_r$.

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

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

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 2.3 to the binomial coefficient and get \((2r)^s\). The product over $k$ becomes \(\binom{2t}{t}\) times

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

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 \(\binom{2r}{r} = 4r\alpha_r\). Putting everything together we find that

\[
\alpha_r = \alpha_r \alpha_t 4^s (1-p) \left( 1 + 2pr' \sum_{k=1}^{2t} \frac{(-1)^{k-1}}{k} \right) \left( \text{mod } p^2 \right).
\]

Using \(4^s (1-p) \equiv 1 - pr' \gamma(\text{mod } p)\) yields our assertion.

\[\square\]

Proof.

In view of congruences (1) it suffices to prove that $F_s(\epsilon_p) \equiv F_1(\epsilon_p) F_{s-1}(\epsilon_p) (\text{mod } p^2)$ for $s = 2$, but we will do it for all $s \geq 2$. Use the notation $\alpha_r = \binom{1/2}{r}$ and Lemma 2.4 to find

\[
F_s(z) = \sum_{r'=0}^{p^s-1} \sum_{t=0}^{(p-1)/2} (\alpha_r \alpha_t)^d z^{pr'+t} \left( 1 - \gamma dr' + 2 pr' \sum_{k=1}^{2t} \frac{(-1)^{k-1}}{k} \right) \left( \text{mod } p^2 \right).
\]

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

\[
F_s(z) \equiv F_1(z) F_{s-1}(z^p) + pd (G_1(z) - \gamma F_1(z)) \sum_{r'=0}^{p^s-1} r' z^{pr'} \alpha_r^d (\text{mod } p^2)
\]

where

\[
G_1(z) = 2 \sum_{t=0}^{(p-1)/2} \left( \sum_{k=1}^{2t} \frac{(-1)^{k-1}}{k} \right) \alpha_t^d z^t.
\]

In order to arrive at our result we set $z = \epsilon_p$ and show that $G_1(\epsilon_p) \equiv \gamma F_1(\epsilon_p) (\text{mod } p)$. Consider $G_1(\epsilon_p) = 2\Sigma = \Sigma + \Sigma$ as a sum of two (equal) sums over $t$. In one of these we replace $t$ by $(p-1)/2 - t$ and obtain

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

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

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

This equals

\[
\sum_{t=0}^{(p-1)/2} \left( \sum_{k=2t+1}^{p-1} \frac{(-1)^{k-1}}{k} \right) \alpha_t^d \epsilon_p (\text{mod } p).
\]
Thus we obtain after addition of $\Sigma$,

$$G_1(\epsilon_p) \equiv \sum_{t=0}^{(p-1)/2} \left( \sum_{k=1}^{p-1} \frac{(-1)^{k-1}}{k} \right) \alpha_t^d \epsilon_p^t \equiv \left( \sum_{k=1}^{p-1} \frac{(-1)^{k-1}}{k} \right) F_1(\epsilon_p) \pmod{p^2}.$$ 

Application of Lemma 2.2 yields the desired result. \qed

3. The underlying mechanism

The proof of our main result uses a symmetry of the polynomials $F_1(z), G_1(z)$ modulo $p$. We show here how this is forced by the symmetry of the hypergeometric equation. One easily sees that $F_1(z)(\mod p)$ is the unique polynomial of degree $< p/2$ which satisfies our hypergeometric differential equation modulo $p$ and which has constant term $1$. Furthermore, $F_1(z) \log z + G_1(z)$ is another solution modulo $p$. By the symmetry of our equation $z^{(p-1)/2} F_1(1/z)$ is also a polynomial solution modulo $p$. Hence, by uniqueness of $F_1$, $z^{(p-1)/2} F_1(1/z) \equiv \lambda F_1(z)(\mod p)$ for some $\lambda$. To determine $\lambda$ 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 $F_1(z)$ is a reciprocal or anti-reciprocal polynomial. We observe that $z^{(p-1)/2} F_1(1/z) \log(1/z) + z^{(p-1)/2} G_1(1/z)$ is also a mod $p$ solution. Multiply by $\epsilon_p$ and add $F_1(z) \log z + G_1(z)$. We find the new solution $G_1(z) + \epsilon_p z^{(p-1)/2} G_1(1/z)$ which is a polynomial solution. Hence it equals $\mu F_1(z)$ for some $\mu$. To find the value of $\mu$ we set $z = 0$. The constant term of $G_1(z)$ is $0$ and the constant term of $\epsilon_p z^{(p-1)/2} G_1(1/z)$ is the leading term of $\epsilon_p G_1(z)$, which is $2 \sum_{j=1}^{p-1} \frac{(-1)^{j-1}}{j}$, hence $2\gamma$ by Lemma 2.2 Using $F_1(0) = 1$ we conclude that $\mu = 2\gamma$. Now set $z = \epsilon_p$ in

$$\epsilon_p z^{(p-1)/2} G_1(1/z) + G_1(z) \equiv 2\gamma F_1(z)(\mod p)$$

and we obtain that $G_1(\epsilon_p) = \gamma F_1(\epsilon_p)$, the key step in the proof of our theorem.

References

[1] C. Babbage, Demonstration of a theorem relating to prime numbers, The Edinburgh Philosophical Journal 1 (1819): 46–49.
[2] B. Dwork, $p$-adic cycles, Publications mathématiques de l’I.H.É.S., tome 37 (1969), p. 27–115.
[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. 4e série, tome 6, 3 (1973), p. 295–316.
[4] G. Eisenstein, Neue Gattung zahlentheoret. Funktionen, die v. 2 Elementen abhängen und durch gewisse lineare Funktional-Gleichungen definiert werden, Bericht über die zur Bekanntmachung geeigneten Verhandlungen der Königl. Preuß. Akademie der Wissenschaften zu Berlin 1850, 36–42.
[5] I. Gessel, Some congruences for Apéry numbers, J. Number Theory, 14 (1982), 362–368.
[6] E. L. Ince, Ordinary Differential Equations, Dover Publications, New York, 1944. viii+558 pp.
[7] L. Long, F.-T. Tu, N. Yui, W. Zudilin, Supercongruences for rigid hypergeometric Calabi-Yau threefolds, Preprint arXiv:1705.01663 [math.NT].
[8] R. Osburn, A. Straub, W. Zudilin, A modular supercongruence for $\zeta(F_2)$: an Apéry-like story, to appear in Annales de l’Institut Fourier, also in Preprint arXiv:1701.04998 [math.NT].
[9] J. Wolstenholme, On certain properties of prime numbers, The Quarterly Journal of Pure and Applied Mathematics, 5 (1862): 35–39.
