View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Elsevier - Publisher Connector

Available online at www.sciencedirect.com

SCIENCE DIRECT®

ELSEVIER

Journal of Combinatorial Theory, Series A 113 (2006) 851–865

Journal of Combinatorial Theory Series A

www.elsevier.com/locate/jcta

Catalan and Apéry numbers in residue classes

Moubariz Z. Garaev[a], Florian Luca[a], Igor E. Shparlinski[b]

[a] *Instituto de Matemáticas, Universidad Nacional Autónoma de México, C.P. 58089, Morelia, Michoacán, México*

[b] *Department of Computing, Macquarie University, Sydney, NSW 2109, Australia*

Received 24 November 2004

Available online 3 October 2005

Abstract

We estimate character sums with Catalan numbers and middle binomial coefficients modulo a prime p. We use this bound to show that the first at most $p^{13/2}(\log p)^6$ elements of each sequence already fall in all residue classes modulo every sufficiently large p, which improves the previously known result requiring $p^{O(p)}$ elements. We also study, using a different technique, similar questions for sequences satisfying polynomial recurrence relations like the Apéry numbers. We show that such sequences form a finite additive basis modulo p for every sufficiently large prime p.

© 2005 Elsevier Inc. All rights reserved.

Keywords: Catalan numbers; Apéry numbers; Congruences; Bounds for character sums

1. Introduction

Let p be an odd prime. In this paper, we study the distribution modulo p of *middle binomial coefficients*

$$b_n = \binom{2n}{n}, \qquad n = 0, 1, \ldots$$

and *Catalan numbers*

$$c_n = \frac{1}{n+1}\binom{2n}{n}, \qquad n = 0, 1, \ldots,$$

where as usual we define $0! = 1$.

E-mail addresses: garaev@matmor.unam.mx (M.Z. Garaev), fluca@matmor.unam.mx (F. Luca), igor@ics.mq.edu.au (I.E. Shparlinski).

0097-3165/$ - see front matter © 2005 Elsevier Inc. All rights reserved.

doi:10.1016/j.jcta.2005.08.003

We estimate the number of solutions of certain congruences with middle binomial coefficients and Catalan numbers. In particular, we show that both b_n and c_n take on all residue classes modulo a sufficiently large p.

These results are used to estimate, both "individually" and "on average", character sums

$$S(\chi; H, N) = \sum_{n=H+1}^{H+N} \chi(b_n),$$

$$T(\chi; H, N) = \sum_{n=H+1}^{H+N} \chi(c_n),$$

where χ is a multiplicative character of $\mathbb{F}_p$.

The method we use is similar to that of [8,9] to estimate character and exponential sums with $n!$. Accordingly, our bounds look very similar. However, using the *Lucas theorem*

$$b_n \equiv \prod_{i=0}^{m-1} b_{t_i} \pmod p, \tag{1}$$

where $n = t_0 + \cdots + t_{m-1} p^{m-1}$ is the p-ary representation of n, we are able to get some results for b_n and c_n that are not known for $n!$ and are in fact not even likely to be true for $n!$. In particular, it is shown in [1] that for infinitely many primes p, at least $(\log\log p)^{1+o(1)}$ residue classes modulo p are not represented by $n! \pmod p$ and it is conjectured in Section **F11** in [11] that about p/e residue classes are missing among the values $n! \pmod p$. Here, we show that each of the sequences b_n and c_n covers all residue classes modulo p even with $n \leqslant p^{13/2}(\log p)^6$. This substantially improves the previously known result of Berend and Harmse [2] where the same statement is shown for integers $n \leqslant p^m$ with m of order p.

Our proof also implies that for $1 \leqslant n \leqslant p^7$, the values of b_n and c_n fall in each nonzero residue class modulo p asymptotically the same number of times, namely $\big(2^{-7} + o(1)\big) p^6$ times.

We also study the number of distinct residue classes modulo p of a *polynomially recurrence sequence* (**PR**-sequence for short). Recall that a **PR**-sequence $(u_n)_{n \geqslant 0}$ is a sequence of integers such that there exist a positive integer ℓ and $\ell + 1$ polynomials $f_i(X) \in \mathbb{Z}[X]$ for $i = 0, \ldots, \ell$, not all zero, such that the recurrence relation

$$\sum_{i=0}^{\ell} f_i(n) u_{n+\ell-i} = 0 \tag{2}$$

holds for all $n \geqslant 0$. We also say that $(u_n)_{n \geqslant 0}$ is a **PR**-sequence of type (ℓ, d) if it satisfies Eq. (2) with

$$\max\{\deg f_i \ : \ i = 0, \ldots, \ell\} \leqslant d.$$

We show that if $(u_n)_{n \geqslant 0}$ is a **PR**-sequence of type (ℓ, d) which is not a linear recurrence sequence for all sufficiently large n, then for any large prime p the number of residue classes modulo p represented by $(u_n)_{n \geqslant 0}$ exceeds cp^{β}, where $c > 0$ is a constant depending on the sequence and $\beta > 0$ is a constant depending only on ℓ and d.

We say that $(u_n)_{n \geqslant 0}$ has the *Lucas property* if for every prime p,

$$u_n \equiv \prod_{i=0}^{m-1} u_{t_i} \pmod p, \tag{3}$$

where

$$n = t_0 + \cdots + t_{m-1} p^{m-1}, \quad 0 \leqslant t_0, \ldots, t_{m-1} \leqslant p-1,$$

is the p-ary representation of n.

If $(u_n)_{n \geqslant 0}$ is a **PR**-sequence (which does not eventually become a linear recurrence sequence) which has the *Lucas property*, then we combine the above bound on the value set of $(u_n)_{n \geqslant 0}$ modulo p with the ingenious result of Bourgain et al. [3] to study a variant of the *Waring problem* modulo p for this sequence. We also show that these residue classes modulo p represented by $(u_n)_{n \geqslant 0}$ are in some sense "densely" distributed.

In particular, we apply our results to study *power sums of binomial coefficients*

$$b_{\nu,n} = \sum_{k=0}^{n} \binom{n}{k}^{\nu}, \quad n = 0, 1, \ldots,$$

where $\nu \geqslant 2$ is a fixed positive integer, as well as to the *Apéry numbers*

$$a_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2, \quad n = 0, 1, \ldots,$$

in residue classes modulo p. Note that $b_{2,n} = b_n$, so in a sense the study of the numbers $b_{\nu,n}$ modulo p may be seen as an extension of the study of the numbers b_n modulo p. We recall that both $(a_n)_{n \geqslant 0}$ and power sums of binomial coefficients $(b_{\nu,n})_{n \geqslant 0}$ have the Lucas property. Indeed, for the case of the Apéry sequence this is shown in [10]. For the sequence of binomial coefficients $(b_{\nu,n})_{n \geqslant 0}$ this can easily be verified by using a more general form of (1), namely

$$\binom{n}{k} \equiv \prod_{i=0}^{m-1} \binom{t_i}{s_i} \pmod{p}, \tag{4}$$

where $n = t_0 + \cdots + t_{m-1} p^{m-1}$ and $k = s_0 + \cdots + s_{m-1} p^{m-1}$ are the p-ary representations of n and k (here, we assume that m is large enough so that the above representations hold; in particular, one of t_{m-1} or s_{m-1} may be zero). It can also be derived from the more general Theorem 3 of McIntosh [15].

Furthermore, $(a_n)_{n \geqslant 0}$ satisfies the recurrence

$$a_n n^3 - a_{n-1}(34n^3 - 51n^2 + 27n - 5) + a_{n-2}(n-1)^3 = 0 \tag{5}$$

for every $n = 2, 3, \ldots$, with the initial values $a_0 = 1$, $a_1 = 5$. It is known that for a fixed ν the sequence $(b_{\nu,n})_{n \geqslant 0}$ satisfies a recurrence of the form (2) with $\ell = \lfloor (\nu+1)/2 \rfloor$ (see [6,17]). Unfortunately, no upper bound d for the degrees of the polynomials $f_i(X)$ for $i = 0, \ldots, \ell$ has ever been worked out specifically, although it may be possible to deduce it by a closer examination of the proofs in [6,17].

Our results apply also to the case when the sequence $b_{\nu,n}$ is replaced by

$$\widetilde{b}_{\nu,n} = \sum_{k=-n}^{n} (-1)^k \binom{2n}{n+k}^{\nu},$$

again for a fixed $\nu \geqslant 2$, as this sequence is both **PR** by the results from [14], and Lucas by the results from [15].

Throughout the paper, the implied constants in symbols 'O', '$\ll$' and '$\gg$' may occasionally, where obvious, depend on some integer parameters m, r, s and v and also on the particular sequence under consideration and are absolute otherwise. We recall that $U \ll V$, $V \gg U$ and $U = O(V)$ are all equivalent to the inequality $|U| \leqslant cV$ with some constant $c > 0$.

2. Catalan numbers

2.1. Bounds of character sums

Let $\mathcal{X}$ denote the set of multiplicative characters of the multiplicative group $\mathbb{F}_p^*$ and let $\mathcal{X}^* = \mathcal{X} \backslash \{\chi_0\}$ be the set of nonprincipal characters.

We start with estimating individual sums. It is clear that $b_n c_n \not\equiv 0 \pmod p$ for $0 \leqslant n < p/2$, so we start with estimating character sums over this interval.

Theorem 1. *Let H and N be integers with $0 \leqslant H < H + N < p/2$. Then the following bound holds*:

$$\max_{\chi \in \mathcal{X}^*} \{|S(\chi; H, N)|, |T(\chi; H, N)|\} \ll N^{3/4} p^{1/8} (\log p)^{1/4}.$$

Proof. For any integer $k \geqslant 0$, we have

$$S(\chi; H, N) = \sum_{n=H+1}^{H+N} \chi(b_{n+k}) + O(k).$$

Therefore, for any integer K with $1 \leqslant K < p/2$, we have

$$S(\chi, H, N) = \frac{1}{K} W + O(K), \tag{6}$$

where

$$W = \sum_{k=0}^{K-1} \sum_{n=H+1}^{H+N} \chi(b_{n+k}) = \sum_{n=H+1}^{H+N} \sum_{k=0}^{K-1} \chi\left(2^k b_n \prod_{i=1}^{k} \frac{2n+2i-1}{n+i}\right)$$
$$= \sum_{n=H+1}^{H+N} \chi(b_n) \sum_{k=0}^{K-1} \chi\left(2^k \prod_{i=1}^{k} \frac{2n+2i-1}{n+i}\right)$$

(note that $1 \leqslant H + 1 < H + N + K < p$ so the above product is well-defined modulo p).

We recall that $|z|^2 = z\overline{z}$ for any complex number z, and that $\overline{\chi}(a) = \chi(a^{-1})$ holds for every integer $a \not\equiv 0 \pmod p$, where $\overline{\chi}$ is the conjugate character of χ. Therefore, applying the Cauchy inequality, we derive

$$|W|^2 \leqslant N \sum_{n=H+1}^{H+N} \left| \sum_{k=0}^{K-1} \chi\left(2^k \prod_{i=1}^{k} \frac{2n+2i-1}{n+i}\right) \right|^2$$
$$= N \sum_{k,m=0}^{K-1} \sum_{n=H+1}^{H+N}{}^{*} \chi\left(\Psi_{k,m}(n)\right), \tag{7}$$

where

$$\Psi_{k,m}(X) = 2^{k-m} \prod_{i=1}^{k} \frac{2X+2i-1}{X+i} \prod_{j=1}^{m} \frac{X+j}{2X+2j-1} \tag{8}$$

and Σ^* means that the poles of $\Psi_{k,m}(X)$ are excluded from the summation.

Clearly, if $K < p$ then, unless $k = m$, the rational function $\Psi_{k,m}(X)$, has at least one simple root or pole, and thus is not a power of any other rational function modulo p.

For the $O(K)$ choices of $0 \leqslant k = m \leqslant K-1$, we estimate the sum over n trivially as N.

For the other $O(K^2)$ choices of $0 \leqslant k, m \leqslant K-1$, using the Weil bound given in Example 12 of Appendix 5 of [18] (see also [12, Theorem 3 of Chapter 6], or [13, Theorem 5.41 and the comments to Chapter 5]), we see that, because $\chi \in \mathcal{X}^*$,

$$\sum_{n=0}^{p-1}{}^{*} \chi\left(\Psi_{k,m}(n)\right) \mathbf{e}(n) = O(Kp^{1/2}),$$

where $\mathbf{e}(z) = \exp(2\pi\imath z/p)$ with $\imath = \sqrt{-1}$, and as before Σ^* means that the poles of $\Psi_{k,m}(X)$ are excluded from the summation. Therefore, by the standard reduction of incomplete sums to complete ones (see [5]), we deduce

$$\sum_{n=H+1}^{H+N}{}^{*} \chi\left(\Psi_{k,m}(n)\right) = O(Kp^{1/2}\log p).$$

Putting everything together, we get

$$|W|^2 \ll N\left(KN + K^3 p^{1/2}\log p\right).$$

Therefore, by (6), we derive

$$S(\chi, H, N) \ll NK^{-1/2} + K^{1/2}N^{1/2}p^{1/4}(\log p)^{1/2} + K.$$

Taking $K = \lfloor N^{1/2}p^{-1/4}(\log p)^{-1/2}\rfloor$, we obtain the desired bound for the sums $S(\chi, H, N)$.

The sums $T(\chi, H, N)$ can be estimated completely analogously. □

We remark that it trivially follows from (7) that

$$|W|^2 \leqslant N \sum_{n=0}^{p-K} \left| \sum_{k=0}^{K-1} \chi\left(2^k \prod_{i=1}^{k} \frac{2n+2i-1}{n+i}\right)\right|^2.$$

Hence, we apply the Weil bound for complete sums which leads us to the estimate

$$\sum_{n=0}^{p-K} \chi\left(\Psi_{k,m}(n)\right) = \sum_{n=0}^{p-1}{}^{*} \chi\left(\Psi_{k,m}(n)\right) + O(K) = O(Kp^{1/2}),$$

which in turn yields the bound

$$|W|^2 \ll N\left(Kp + K^3 p^{1/2}\right).$$

Taking $K = \lfloor N^{1/2} p^{-1/4} \rfloor$, we derive

$$\max_{\chi \in \mathcal{X}^*} \{|S(\chi; H, N)|, |T(\chi; H, N)|\} \ll p^{7/8}, \tag{9}$$

which is a little better than the bound of Theorem 1 when N is of order close to p.

We also need some estimates "on average".

Theorem 2. *Let H and N be integers with $0 \leqslant H < H + N < p/2$. For any integer $\nu \geqslant 1$ the following bound holds*:

$$\max \left\{ \sum_{\chi \in \mathcal{X}} |S(\chi, H, N)|^{2\nu}, \sum_{\chi \in \mathcal{X}} |T(\chi, H, N)|^{2\nu} \right\} \ll p N^{2\nu - 1 + 2^{-\nu}}.$$

Proof. We recall the identity

$$\sum_{\chi \in \mathcal{X}} \chi(u) = \begin{cases} 0 & \text{if } u \not\equiv 1 \pmod{p}, \\ p - 1 & \text{if } u \equiv 1 \pmod{p}. \end{cases} \tag{10}$$

We remark that, by (10), we have

$$\sum_{\chi \in \mathcal{X}} |S(\chi, H, N)|^{2\nu} = (p-1) I_\nu(H, N),$$

where $I_\nu(H, N)$ is the number of solutions to the congruence

$$\prod_{i=1}^{\nu} b_{n_i} \equiv \prod_{i=\nu+1}^{2\nu} b_{n_i} \pmod{p}, \qquad H + 1 \leqslant n_1, \ldots, n_{2\nu} \leqslant H + N.$$

We prove by induction on ν that

$$I_\nu(H, N) \ll N^{2\nu - 1 + 2^{-\nu}}.$$

The implied constant above depends on ν. If $\nu = 1$, then arguing as in the proof of Theorem 1, we derive that for any integer K with $1 \leqslant K < p/2$, we have

$$|S(\chi, H, N)|^2 \ll K^{-2} N \sum_{k,m=0}^{K-1} \sum_{n=H+1}^{H+N}{}^{*} \chi\big(\Psi_{k,m}(n)\big) + K^2,$$

where $\Psi_{k,m}(X)$ is given by (8) and as before Σ^* means that the poles of $\Psi_{k,m}(X)$ are excluded from the summation. Therefore,

$$\sum_{\chi \in \mathcal{X}} |S(\chi, H, N)|^2 \ll K^{-2} N \sum_{k,m=0}^{K-1} \sum_{n=H+1}^{H+N}{}^{*} \sum_{\chi \in \mathcal{X}} \chi\big(\Psi_{k,m}(n)\big) + pK^2.$$

Then, from (10), we see that the sum over χ vanishes, unless

$$\Psi_{k,m}(n) \equiv 1 \pmod{p}, \tag{11}$$

in which case it equals $p-1$. For the K pairs (k,m) with $k=m$ there are N possible solutions to (11), while for the other $O(K^2)$ pairs there are $O(K)$ solutions to (11). Thus,

$$\sum_{\chi\in\mathcal{X}} |S(\chi,H,N)|^2 \ll K^{-2}N\left(K^3+KN\right)p + pK^2 = \left(NK+N^2K^{-1}+K^2\right)p.$$

Taking $K=\lfloor N^{1/2}\rfloor$, we deduce

$$I_\nu(H,N) = \frac{1}{p-1}\sum_{\chi\in\mathcal{X}} |S(\chi,H,N)|^2 \ll N^{3/2}.$$

Assume now that $\nu\geqslant 2$ and that

$$I_{\nu-1}(H,N) \ll pN^{2\nu-3+2^{-\nu+1}}.$$

We fix some $K<N$ and note that by the Cauchy inequality, we have

$$\left|\sum_{n=H+1}^{H+N}\chi(b_n)\right|^2 = \left|\sum_{k=1}^{K}\sum_{H+(k-1)N/K<m\leqslant H+kN/K}\chi(b_m)\right|^2 \leqslant K\sum_{k=1}^{K}\left|\sum_{H+(k-1)N/K<m\leqslant H+kN/K}\chi(b_m)\right|^2.$$

Therefore,

$$\sum_{\chi\in\mathcal{X}} |S(\chi,H,N)|^{2\nu} \leqslant K\sum_{k=1}^{K}\sum_{\chi\in\mathcal{X}}\left|\sum_{H+(k-1)N/K<m\leqslant H+kN/K}\chi(b_m)\right|^2 \times\left|\sum_{n=H+1}^{H+N}\chi(b_n)\right|^{2\nu-2} = K\widetilde{I}_\nu(K,H,N),$$

where $\widetilde{I}_\nu(K,H,N)$ is the number of solutions to the congruence

$$b_{m_1}\prod_{i=1}^{\nu-1} b_{n_i} \equiv b_{m_2}\prod_{i=\nu}^{2\nu-2} b_{n_i} \pmod p$$

with $H+1\leqslant n_1,\dots,n_{2\nu-2}\leqslant H+N$, and $H+(k-1)N/K<m_1,m_2\leqslant H+kN/K$ for some $k=1,\dots,K$. For each of the N pairs (m_1,m_2) with $m_1=m_2$ there are exactly $I_{\nu-1}(H,N)$ solutions. We also see that if $n_1,\dots,n_{2\nu-2}$ are given then for each fixed value of $r=m_1-m_2$ there are no more than $|r|$ solutions in m_1,m_2 (because at least one of m_1 or m_2 satisfies a nontrivial polynomial congruence of degree $|r|$). Certainly, $r=O(N/K)$. Putting everything together and using the induction assumption, we obtain

$$\widetilde{I}_\nu(K,H,N) \ll NI_{\nu-1}(H,N) + (N/K)^2N^{2\nu-2} = N^{2\nu-2+2^{-\nu+1}} + N^{2\nu}K^{-2}.$$

Therefore $I_\nu(H,N) \ll KN^{2\nu-2+2^{-\nu+1}} + N^{2\nu}K^{-1}$. Choosing $K = \lceil N^{1-2^{-\nu}} \rceil$, we obtain the desired bound for the sums $S(\chi, H, N)$.

The sums $T(\chi, H, N)$ can be estimated completely analogously. □

2.2. Distribution in residue classes

Theorem 3. *For all sufficiently large primes p and every integer λ there exist positive integers $r, s \leqslant p^{13/2}(\log p)^6$ such that $b_r \equiv c_s \equiv \lambda \pmod p$.*

Proof. If $\lambda \equiv 0 \pmod p$, we simply take $r = s = (p+1)/2$.

We now assume that $\lambda \not\equiv 0 \pmod p$.

We put $N = \lfloor p^{1/2}(\log p)^6 \rfloor$ and consider the set $\mathcal{N}$ of positive integers n whose p-ary representation is of the form

$$n = n_0 + \cdots + n_6 p^6, \quad 0 \leqslant n_0, \ldots, n_5 \leqslant \frac{p-1}{2}, \quad 0 \leqslant n_6 \leqslant N. \tag{12}$$

Let $Q(N, \lambda)$ be the number of solutions to the congruence

$$b_n \equiv \lambda \pmod p, \quad n \in \mathcal{N}.$$

By (10), we have

$$Q(N,\lambda) = \frac{1}{p-1} \sum_{n\in\mathcal{N}} \sum_{\chi\in\mathcal{X}} \chi(\lambda^{-1} b_n) = \frac{1}{p-1} \sum_{\chi\in\mathcal{X}} \chi(\lambda^{-1}) \sum_{n\in\mathcal{N}} \chi(b_n).$$

Separating the term

$$\frac{\#\mathcal{N}}{p-1} = \frac{(N+1)(p+1)^6}{2^6(p-1)},$$

corresponding to the principal character χ_0, we obtain

$$\left| Q(N,\lambda) - \frac{(N+1)(p+1)^6}{2^6(p-1)} \right| \leqslant \frac{1}{p-1} \sum_{\chi\in\mathcal{X}^*} \left| \sum_{n\in\mathcal{N}} \chi(b_n) \right|.$$

We now see that, by (1),

$$\sum_{n\in\mathcal{N}} \chi(b_n) = \big(S(\chi; 0, (p-1)/2) + 1\big)^6 \big(S(\chi; 0, N) + 1\big)$$

(since $\chi(b_0) = \chi(1) = 1$).

Hence, applying Theorem 1, and then Theorem 2 with $\nu = 1$, we obtain

$$\frac{1}{p-1} \sum_{\chi\in\mathcal{X}^*} \left| \sum_{n\in\mathcal{N}} \chi(b_n) \right|$$
$$\leqslant \frac{1}{p-1} \sum_{\chi\in\mathcal{X}^*} \big(|S(\chi; 0, (p-1)/2)| + 1\big)^6 \big(|S(\chi; 0, N)| + 1\big)$$

$$\ll \frac{1}{p-1} N^{3/4} p^{1/8} (\log p)^{1/4} \left(p^{7/8} (\log p)^{1/4}\right)^4$$
$$\times \sum_{\chi \in \mathcal{X}^*} \left(|S(\chi; 0, (p-1)/2)|^2 + 1\right)$$
$$\ll \frac{1}{p-1} N^{3/4} p^{1/8} (\log p)^{1/4} \left(p^{7/8} (\log p)^{1/4}\right)^4 p^{5/2}$$
$$= N^{3/4} p^{41/8} (\log p)^{5/4}.$$

Therefore,

$$Q(N,\lambda) = \frac{(N+1)(p+1)^5}{2^6} + O\left(N^{3/4} p^{41/8} (\log p)^{5/4}\right)$$
$$= \frac{(N+1)(p+1)^5}{2^6} \left(1 + O\left(N^{-1/4} p^{1/8} (\log p)^{5/4}\right)\right). \tag{13}$$

Recalling the choice of N, we see that $Q(N,\lambda) > 0$ for sufficiently large p. Therefore $b_r \equiv \lambda \pmod p$ for some positive integer $r \leqslant p^6 N \leqslant p^{13/2} (\log p)^6$.

Similar arguments also show that $c_s \equiv \lambda \pmod p$ for some positive integer $s \leqslant p^6 N \leqslant p^{13/2} (\log p)^6$. $\square$

Since $b_n \not\equiv 0 \pmod p$ if and only if the p-ary digits of n are all less than $p/2$, we see from (13) that for every $\lambda \not\equiv 0 \pmod p$ the number of solutions of each of the congruences

$$b_n \equiv \lambda \pmod p \quad \text{and} \quad c_n \equiv \lambda \pmod p,$$

for $0 \leqslant n \leqslant p^7 - 1$ is $2^{-7} p^6 \left(1 + O\left(p^{-1/8} (\log p)^{5/4}\right)\right)$. In fact, using (9), this can be slightly improved to $2^{-7} p^6 \left(1 + O\left(p^{-1/8}\right)\right)$.

3. PR-sequences

3.1. The set of residues

We start with the following property of **PR**-sequences.

Lemma 4. *Let $(u_n^{(j)})_{n \geqslant 0}$, be* **PR**-*sequences of integers of type (ℓ_j, d), with $\ell_j \leqslant \ell$ for $j = 1, \dots, m$. Let*

$$v_n = \sum_{j=1}^{m} \lambda_j u_n^{(j)}, \quad n = 0, 1, \dots,$$

where λ_j are arbitrary integers. Then $(v_n)_{n \geqslant 0}$ is a **PR**-*sequence of integers of type $(2m\ell, 2dm\ell)$.*

Proof. Assume that the sequences $(u_n^{(j)})_{n \geqslant 0}$ satisfy the recurrences

$$\sum_{i=0}^{\ell_j} f_i^{(j)}(n) u_{n+\ell_j - i}^{(j)} = 0 \tag{14}$$

with $f_i^j(X) \in \mathbb{Z}[X]$ for $i = 0, \dots, \ell_j$, and where for each $j = 1, \dots, m$ not all polynomials $f_i^{(j)}(X)$, $i = 0, \dots, \ell_j$, are zero. Furthermore, we assume that $\ell_j \leqslant \ell$ for $j = 0, \dots, m$, and that the degrees of all the polynomials $f_i^{(j)}$ are at most d.

Without loss of generality, we may assume that $\lambda_j \neq 0$ and that $f_0^{(j)}(X)$ is not the zero polynomial for $j = 1, \dots, m$.

It is enough to show that for $t = 2m\ell$ there exist $t + 1$ polynomials $F_i(X) \in \mathbb{Z}[X]$, not all zero and of degrees at most $D = 2dm\ell$, such that

$$\sum_{i=0}^{t} F_i(n) v_{n+t-i} = 0, \quad n = 0, 1, \dots .$$

By replacing the sequence $(u_n^{(j)})_{n \geqslant 0}$ by the sequence $(\lambda_j u_n^{(j)})_{n \geqslant 1}$, we may assume that $\lambda_j = 1$ for all $j = 1, \dots, m$. We now show that for each $h \geqslant 0$, we have a relation of the form

$$u_{n+h}^{(j)} = \sum_{i=0}^{\ell_j - 1} g_{i,j,h}(n) u_{n+i}^{(j)}, \tag{15}$$

where $g_{i,j,h}(X)$ are rational functions with the same denominator such that both the numerator and denominator have degrees at most $\max\{0, (h - \ell_j + 1)d\}$. Indeed, if $h \leqslant \ell_j - 1$, we set $g_{i,j,h}(X) = 1$ if $i = j$ and we set $g_{i,j,h}(X) = 0$ otherwise. Then relations (15) are fulfilled. If $h = \ell_j$, we simply set $g_{i,j,\ell_j}(X) = -f_{\ell_j - i}^{(j)}(X)/f_0^{(j)}(X)$ and relation (15) is then a consequence of the recurrence (14). We now proceed by induction on h. Assuming that (15) holds for h, then

$$\begin{aligned} u_{n+h+1}^{(j)} &= \sum_{i=0}^{\ell_j - 1} g_{i,j,h}(n+1) u_{n+1+i}^{(j)} \\ &= \sum_{i=0}^{\ell_j - 2} g_{i,j,h}(n+1) u_{n+1+i}^{(j)} + g_{\ell_j - 1,j,h}(n+1) u_{n+\ell_j}^{(j)} \\ &= g_{\ell_j - 1,j,h}(n+1) g_{0,j,\ell_j}(n) u_n^{(j)} \\ &\quad + \sum_{i=1}^{\ell_j - 1} \bigl(g_{i-1,j,h}(n+1) + g_{\ell_j - 1,j,h}(n+1) g_{i,j,\ell_j}(n)\bigr) u_{n+i}^{(j)} \end{aligned}$$

and so (15) holds for $h + 1$ if we set

$$g_{0,j,h+1}(X) = g_{\ell_j - 1,j,h}(X+1) g_{0,j,\ell_j}(X)$$

and

$$g_{i,j,h+1}(X) = g_{i-1,j,h}(X+1) + g_{\ell_j - 1,j,h}(X+1) g_{i,j,\ell_j}(X), \quad i = 1, \dots, \ell_j - 1.$$

One can also see from the above formulas, that we may assume that for the same values of j and h, the rational functions $g_{i,j,\ell_j}(X)$, $i = 1, \dots, \ell_j - 1$ have the same denominator.

The assertion about the degrees is now obvious.

Equipped with the representation (15), it follows that if $F_i(X) \in \mathbb{Z}[X]$ for $i = 0, \ldots, t$ are any polynomials, then

$$\sum_{i=0}^{n} F_i(n) v_{n+t-i} = \sum_{h=0}^{t} v_{n+h} F_{t-h}(n)$$

$$= \sum_{j=1}^{m} \sum_{i=0}^{\ell_j - 1} \left(\sum_{h=0}^{t} g_{i,j,h}(n) F_{t-h}(n) \right) u_{n+i}^{(j)}.$$

In order for the above expression to be zero, it suffices that

$$\sum_{h=0}^{t} g_{i,j,h}(X) F_{t-h}(X) = 0 \tag{16}$$

holds identically over $\mathbb{Z}[X]$, for all $j = 1, \ldots, m$ and $i = 0, \ldots, k_j - 1$.

Assume that $F_i(X) \in \mathbb{Z}[X]$, $i = 0, \ldots, t$ are polynomials of degree at most D. Then the left-hand side of (16) is a rational function whose numerator is polynomial of degree at most $td + D$. Thus, (16) leads to a homogeneous system of

$$(td + D + 1) \sum_{j=1}^{m} \ell_j \leqslant (td + D + 1) m\ell$$

linear equations in $t(D + 1)$ variables. This system has a nontrivial solution provided that

$$(t + 1)(D + 1) > (td + D + 1) m\ell.$$

Recalling that $t = 2m\ell$ we see that $D = td = 2dm\ell$ satisfies this inequality, which completes the proof. □

Recall that $(u_n)_{n \geqslant 0}$ is a linear recurrence sequence if and only if $(u_n)_{n \geqslant 0}$ is a **PR**-sequence having a recurrence whose coefficients are constant polynomials (not all zero). We say that $(u_n)_{n \geqslant 0}$ is a *proper* **PR**-*sequence* if it is a **PR**-sequence and there is no n_0, such that $(u_n)_{n \geqslant n_0}$ is a linear recurrence sequence.

Theorem 5. *Let $(u_n)_{n \geqslant 0}$ be a proper* **PR**-*sequence of integers of type (ℓ, d). For a prime number p we put*

$$\mathcal{V}(p) = \{u_n \pmod p \ : \ n = 0, 1, \ldots\}.$$

Then the estimate $\#\mathcal{V}(p) \gg p^{\beta}$ holds, where

$$\beta = \frac{1}{2d\ell(\ell + 1)^2}.$$

Proof. Write

$$\sum_{i=0}^{\ell} f_i(n) u_{n+\ell-i} = \sum_{j=0}^{D} L_j(u_n, \ldots, u_{n+\ell}) n^j,$$

where $L_j(X_0,\dots,X_\ell)$ are linear forms with integer coefficients. Since at least one of the polynomials $f_i(X)$ is nonzero, it follows that there exists j_0 such that L_{j_0} is not the zero form. We write $v_n = L_{j_0}(u_n,\dots,u_{n+\ell})$ and apply Lemma 4 to deduce that there exists a recurrence

$$\sum_{i=1}^{t} g_i(X)v_{n+t-i} = 0, \quad n = 0,1,\dots, \tag{17}$$

where $g_i(X) \in \mathbb{Z}[X]$ are polynomials for $i = 0,\dots,t \leqslant 2\ell(\ell+1)$ of degrees not exceeding $D = 2d\ell(\ell+1)$. We assume, without loss of generality, that $g_0(X)g_t(X)$, is not the zero polynomial. Let n_0 the largest positive integer root of $g_0(X)g_t(X)$ (if this polynomial does not have positive integer roots we take $n_0 = 0$), and let δ be such that the inequality $n < \delta y^{1/D}$ implies that $|g_t(n)| < y$ holds for all $y \geqslant n_0 + 1$. Put $\mathcal{I} = \mathbb{Z} \cap [n_0 + 1, \delta p^{1/D} - t]$, and assume that p is a large enough prime so that $\mathcal{I}$ is not empty.

For each $n \in \mathcal{I}$, the recurrence (2) gives a relation for n of the type

$$f_0(n)w_0 + \cdots + f_\ell(n)w_\ell \equiv 0 \pmod p, \tag{18}$$

where the vector $(w_0,\dots,w_\ell) \equiv (u_{n+\ell},\dots,u_n) \pmod p$ is an element of $\mathcal{V}(p)^{\ell+1}$, so it can take at most $\#\mathcal{V}(p)^{\ell+1}$ values.

Whenever $(w_0,\dots,w_\ell)$ is such that the above relation (18) is a nontrivial polynomial relation modulo p for n, the number of values of n which satisfy (18) is at most D. Hence, there are at most $D\#\mathcal{V}(p)^{\ell+1}$ values of $n \in \mathcal{I}$ for which the above polynomial relation (18) is nontrivial.

If the relation (18) is trivial, then the polynomial

$$\sum_{j=0}^{D} L_j(w_0,\dots,w_\ell)X^j \in \mathbb{Z}[X]$$

is identically zero modulo p. In particular,

$$L_{j_0}(u_n,\dots,u_{n+\ell}) \equiv 0 \pmod p. \tag{19}$$

Assume that (19) holds for t consecutive values of $n \in \mathcal{I}$. Let those values of n be $m+1,\dots,m+t$. Evaluating the formula (17) in $n = m$ and reducing modulo p, we get

$$g_t(m)v_m \equiv 0 \pmod p.$$

Since $m \in \mathcal{I}$, it follows that $|g_t(m)| < p$ and $g_t(m) \neq 0$. Hence, the above congruence implies that $v_m \equiv 0 \pmod p$. Continuing in this way, we see that $v_i \equiv 0 \pmod p$, for all integers $n_0 < i \leqslant m$. In particular, assuming that p is large enough, we see that in this case $v_i = 0$ for $i = n_0 + 1,\dots,n_0 + t - 1$. However, this implies that $v_i = 0$ for all $i > n_0$, which means that $(u_n)_{n \geqslant n_0+1}$ is a linear recurrence sequence, contradicting our assumption. Thus, the congruence (19) cannot hold for t consecutive values of $n \in \mathcal{I}$. This shows that one out of every t elements in $\mathcal{I}$ has the property that its associated congruence (18) is not trivial. In turn, this shows that

$$D\#\mathcal{V}(p)^{\ell+1} \geqslant \left\lfloor \frac{\#\mathcal{I}}{t} \right\rfloor \gg p^{1/D},$$

giving the claimed result. □

Remark 6. In some instances, one may deduce a better inequality. For instance, assume that $(u_n)_{n\geqslant 0}$ satisfies the recurrence (2) where the polynomials $f_0(X), \dots, f_\ell(X)$ are linearly independent over $\mathbb{Q}$. Here, we no longer assume that $(u_n)_{n\geqslant 0}$ is a proper **PR**-sequence. It is then clear that they remain linearly independent over the finite field with p elements $\mathbb{Z}_p$ if p is sufficiently large. Furthermore, in this case the relation (18) cannot be trivial. The above argument now easily yields a stronger and more general bound

$$\#\mathcal{V}(N;\, p) \gg (\min\{p, N\})^{1/(\ell+1)},$$

where

$$\mathcal{V}(N;\, p) = \{u_n \pmod p \;:\; n = 0, \dots, N-1\}.$$

Using recurrence (5) and observing that the three polynomials $f_0(X) = X^3$, $f_1(X) = 34X^3 - 51X^2 + 27X - 5$, $f_2(X) = (X-1)^3$ are linearly independent over $\mathbb{Q}$, one uses the argument of Remark 6 to derive the inequality

$$\#\mathcal{V}(p, N) \geqslant \left(\frac{N-2}{3}\right)^{1/3}$$

if $N \leqslant p$ for the case of the Apéry numbers.

In order to be able to deal with the sequences $(b_{v,n})_{n\geqslant 1}$ and $(\widetilde{b}_{v,n})_{n\geqslant 0}$, it suffices to show that they are not linear recurrence sequences from some point on. Note that we need that $v \geqslant 2$, otherwise $b_{1,n} = 2^n$ and $\widetilde{b}_{1,n} = 0$. When $v = 2$, we have $b_{2,n} = b_n$, thus Remark 6 applies again (in any case for this sequence, stronger results are obtained in Section 2). Assume now that $v \geqslant 3$.

Since

$$\binom{n}{k} \leqslant \binom{n}{\lfloor n/2 \rfloor} \sim \frac{2^n}{n^{1/2}}, \quad k = 0, \dots, n,$$

it follows easily that

$$\frac{2^{vn}}{n^{v/2}} \ll b_v(n) \ll \frac{2^{vn}}{n^{v/2-1}}.$$

Furthermore,

$$\widetilde{b}_{v,n} \sim \frac{(2\cos(\pi/2v))^{2nv+v-1}}{\sqrt{v}2^{v-2}(\pi n)^{(v-1)/2}}$$

if $N \leqslant p$for $v \geqslant 2$ (see [4]).

Now the fact that $(b_{v,n})_{n\geqslant 1}$ and $(\widetilde{b}_{v,n})_{n\geqslant 0}$ are not linear recurrence sequences from some point on follows immediately from Theorem 2.6 of Everest et al. [7].

3.2. The Waring problem and distribution of residues

As we have remarked, Apéry numbers $(a_n)_{n\geqslant 0}$ as well as sums of powers of binomial coefficients $(b_{v,n})_{n\geqslant 1}$ and $(\widetilde{b}_{v,n})_{n\geqslant 0}$ are proper **PR**-sequence which also have the Lucas property. Here we show that all such sequences form a finite additive basis modulo p for every sufficiently large prime p.

Theorem 7. *Let $(u_n)_{n\geqslant 0}$ be a proper* **PR***-sequence of integers of type (ℓ, d) with the Lucas property. There exists an absolute constant $c > 0$ such that for $m = \lceil (d\ell)^c \rceil$, $s = \lceil \exp((d\ell)^c) \rceil$, and every sufficiently large prime p, the congruence*

$$u_{n_1} + \cdots + u_{n_s} \equiv \lambda \pmod p$$

has a solution for any integer λ in some nonnegative integers $n_1, \ldots, n_s < p^m$.

Proof. Let $\mathcal{T}$ be a set of the largest possible cardinality of positive integers $t \leqslant p$, such that u_t with $t \in \mathcal{T}$ are pairwise distinct. By Theorem 5, we have $\#\mathcal{T} \gg p^\beta$, where $\beta = 1/2d\ell(\ell+1)^2$. Therefore, by the result of Bourgain et al. [3], there are some positive constants, c_1, c_2, c_3 such that for any $m > \lceil \beta^{c_1} \rceil$ and $\gamma = \exp(-c_2\beta^{-c_3})$, the bound

$$\max_{\gcd(a,p)=1} \left| \sum_{t_0,\ldots,t_{m-1}\in\mathcal{T}} \mathbf{e}(a u_{t_0} \ldots u_{t_{m-1}}) \right| \ll (\#\mathcal{T})^m p^{-\gamma},$$

holds, where, as before, $\mathbf{e}(z) = \exp(2\pi\imath z/p)$ and $\imath = \sqrt{-1}$.

Denoting by $\mathcal{N}$ the set of positive integers n whose p-ary expansion is of the form $n = t_0 + \cdots + t_{m-1}p^{m-1}$ with $t_0, \ldots, t_{m-1} \in \mathcal{T}$, we see, by (3), that the previous bound is equivalent to

$$\max_{\gcd(c,p)=1} \left| \sum_{n\in\mathcal{N}} \mathbf{e}(c u_n) \right| \ll \#\mathcal{N} p^{-\gamma}. \tag{20}$$

From the identity

$$\sum_{c=0}^{p-1} \mathbf{e}(cu) = \begin{cases} 0 & \text{if } u \not\equiv 0 \pmod p, \\ p & \text{if } u \equiv 0 \pmod p, \end{cases}$$

we deduce that the number $Q(\lambda)$ of solutions of the congruence of the theorem with $n_1, \ldots, n_s \in \mathcal{N}$ can be expressed as

$$Q(\lambda) = \frac{1}{p} \sum_{c=0}^{p-1} \sum_{n_1,\ldots,n_s\in\mathcal{N}} \mathbf{e}(c(u_{n_1} + \cdots + u_{n_s} - \lambda))$$
$$= \frac{1}{p} \sum_{c=0}^{p-1} \mathbf{e}(-c\lambda) \left(\sum_{n\in\mathcal{N}} \mathbf{e}(c u_n) \right)^m.$$

Separating the term $(\#\mathcal{N})^s p^{-1}$ corresponding to $c = 0$ and using (20) for the other terms, we derive

$$Q(\lambda) = (\#\mathcal{N})^s p^{-1} + O\left((\#\mathcal{N})^s p^{-\gamma s}\right).$$

Thus, for any $s > \lfloor \gamma^{-1} \rfloor + 1$, we see that $Q(\lambda) > 0$ for all sufficiently large p. Since $\beta^{-1} = 2d\ell(\ell+1)^2 \leqslant 8d\ell^3 \leqslant d^4\ell^3$, we obtain the desired result for an appropriate value of c. $\square$

Very similar ideas also lead to the following result:

Theorem 8. *Let* $(u_n)_{n\geqslant 0}$ *be a proper* **PR***-sequence of integers of type* (ℓ, d) *with the Lucas property. There exists an absolute constant* $c > 0$, *such that for* $m = \lceil (d\ell)^c \rceil$, $\alpha = \exp(-(d\ell)^c)$, *and every sufficiently large prime* p, *the congruence*

$$u_n \equiv \lambda + \eta \pmod p$$

has a solution for every integer λ *in some nonnegative integers* $n < p^m$ *and* $\eta \leqslant p^{1-\alpha}$.

Proof. The proof follows from (20) with any $\alpha < \gamma$ by standard arguments relating exponential sums and the uniformity of distribution properties of sequences (see, for example [16, Corollary 3.11]). □

We see that both Theorems 7 and 8 apply to Apéry numbers $(a_n)_{n\geqslant 0}$ and sums of powers of binomial coefficients $(b_{v,n})_{n\geqslant 1}$ and $(\widetilde{b}_{v,n})_{n\geqslant 0}$.

Acknowledgments

During the preparation of this paper, M. G. and F. L. were supported in part by Grant SEP-CONACYT 46755, and I. S. was supported in part by ARC Grant DP0556431.

References

[1] W.D. Banks, F. Luca, I.E. Shparlinski, H. Stichtenoth, On the value set of $n!$ modulo a prime, Turkish Math. J. 29 (2005) 169–174.
[2] D. Berend, J.E. Harmse, On some arithmetical properties of middle binomial coefficients, Acta Arith. 84 (1998) 31–41.
[3] J. Bourgain, A.A. Glibichuk, S.V. Konyagin, Estimates for the number of sums and products and for exponential sums in fields of prime order, Preprint, 2004.
[4] N.G. De Bruijn, Asymptotic Methods in Analysis, North-Holland, Amsterdam, 1970.
[5] J.H.H. Chalk, Polynomial congruences over incomplete residue systems modulo k, Proc. Kon. Ned. Acad. Wetensch. A 92 (1989) 49–62.
[6] T.W. Cusick, Recurrences for sums of powers of binomial coefficients, J. Combin. Theory Ser. A 52 (1989) 77–83.
[7] G. Everest, A.J. van der Poorten, I.E. Shparlinski, T.B. Ward, Recurrence sequences, Amer. Math. Soc. (2003).
[8] M.Z. Garaev, F. Luca, I.E. Shparlinski, Character sums and congruences with $n!$, Trans. Amer. Math. Soc. 356 (2004) 5089–5102.
[9] M.Z. Garaev, F. Luca, I.E. Shparlinski, Exponential sums and congruences with factorials, J. Reine Angew. Math. 584 (2005) 29–44.
[10] I. Gessel, Some congruences for Apéry numbers, J. Number Theory 14 (1982) 362–368.
[11] R.K. Guy, Unsolved Problems in Number Theory, Springer, New York, 2004.
[12] W.-C.W. Li, Number Theory with Applications, World Scientific, Singapore, 1996.
[13] R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 1997.
[14] R.J. McIntosh, Recurrences for alternating sums of powers of binomial coefficients, J. Combin. Theory Ser. A 63 (1993) 223–233.
[15] R.J. McIntosh, A generalization of a congruential property of Lucas, Amer. Math. Monthly 99 (1992) 231–238.
[16] H. Niederreiter, Random Number Generation and Quasi–Monte Carlo Methods, SIAM, Philadelphia, 1992.
[17] M. Stoll, Bounds for the length of recurrence relations for convolutions of P-recursive sequences, European J. Combin. 18 (1997) 707–712.
[18] A. Weil, Basic Number Theory, Springer, New York, 1974.