DE GRUYTER
OPEN

uniform
distribution
theory

DOI: 10.1515/udt-2016–0017
Unif. Distrib. Theory **11** (2016), no.2, 151–161

SPATIAL EQUIDISTRIBUTION OF BINOMIAL COEFFICIENTS MODULO PRIME POWERS

Guy Barat—Peter J. Grabner †

Dedicated to the memory of Pierre Liardet

ABSTRACT. The spatial distribution of binomial coefficients in residue classes modulo prime powers is studied. It is proved *inter alia* that empirical distribution of the points $(k,m)p^{-m}$ with $0 \le k \le n < p^m$ and $\binom{n}{k} \equiv a \pmod p)^s$ (for $(a,p)=1$) for $m \to \infty$ tends to the Hausdorff measure on the "p-adic Sierpiński gasket", a fractals studied earlier by von Haeseler, Peitgen, and Skordev.

Communicated by Jean Louis Verger-Gaugry

1. Introduction and Results

Binomial coefficients and their number theoretic properties are the subject of a vast number of investigations. For instance, D. Singmaster [11] have studied divisibility properties and proved that for any integer m almost all binomial coefficients are divisible by m in the following sense

$$\lim_{N\to\infty} \frac{2}{N(N+1)} \# \left\{ k,n\,;\, 0 \le k \le n < N \wedge m \mid \binom{n}{k} \right\} = 1.$$

After this it is natural to ask what happens for the remaining set of density 0, or how the binomial coefficients behave after dividing out the highest possible power of m. For prime p, the first question has been answered independently

2010 Mathematics Subject Classification: Primary 11B65; Secondary 11A63.
Keywords: Binomial coefficients, equidistribution.
† This author is supported by the Austrian Science Fund FWF projects F5503 (part of the Special Research Program (SFB) "Quasi-Monte Carlo Methods: Theory and Applications") and W1230 (Doctoral Program "Discrete Mathematics").

in [2] and [5], namely the binomial coefficients not divisible by p are evenly distributed in the prime residue classes modulo p

$$\lim_{N\to\infty} \frac{\#\left\{k,n\,;\,0\le k\le n<N\wedge \binom{n}{k}\equiv a \pmod p\right\}}{\#\left\{k,n\,;\,0\le k\le n<N\wedge \binom{n}{k}\not\equiv 0 \pmod p\right\}} = \frac{1}{p-1} \text{ for } (a,p)=1.$$

The methods used in these two papers are rather different: in [2] multiplicative characters are used, whereas in [5] polynomial congruences over finite fields are applied. Both methods are based on É. Lucas' [10] congruence

$$\binom{n}{k} \equiv \binom{n_0}{k_0}\binom{n_1}{k_1}\cdots\binom{n_L}{k_L} \pmod p,$$

where $n=\sum_{\ell=0}^{L} n_\ell p^\ell$ and $k=\sum_{\ell=0}^{L} k_\ell p^\ell$ are the respective p-adic digital expansions of n and k (with possible leading zeroes in the expansion of k). The result was extended to prime powers in [1] using a generalisation of Lucas' congruence due to A. Granville [7], see Theorem 3. The second question was addressed in the same paper, where it was shown that the p-free parts of the binomial coefficients are uniformly distributed in $\mathbb{Z}_p^*$ (p-adic integers). Notice that the p-free part of an integer n is given by $n_{(p)}=np^{-v_p(n)}$, where v_p denotes the p-adic valuation. The result reads as

$$\lim_{N\to\infty} \frac{2}{N(N+1)} \#\left\{k,n\,;\,0\le k\le n<N\wedge \binom{n}{k}_{(p)} \equiv a \pmod{p^s}\right\}$$
$$= \frac{1}{\phi(p^s)} = \frac{1}{p^{s-1}(p-1)} \tag{1}$$

for all $s\in\mathbb{N}$ and all a not divisible by p; ϕ denotes Euler's totient as usual.

Furthermore, the number of binomial coefficients up to row N which have p-adic valuation j, has been studied by L. Carlitz [3]. This is based on E. E. Kummer's result [9], which states that the p-valuation of $\binom{n}{k}$ equals the number of carries in the subtraction $n-k$ performed in base p. In [1] Carlitz' result could be refined to a precise asymptotic formula; recently L. Spiegelhofer and M. Wallner [12] found expressions for

$$\#\left\{k,n\,;\,0\le k\le n\wedge v_p\left(\binom{n}{k}\right)=j\right\}$$

in terms of the numbers of certain blocks occurring in the digital expansion of n.

Also recently, F. Greinecker [8] could prove that binomial coefficients, Stirling numbers, and more generally number schemes satisfying generalisations of Lucas' congruence are spatially uniformly distributed modulo p in a sense that we will make precise below.

The present paper exhibits detailed properties of the distribution of binomial coefficients in residue classes modulo prime powers in the respects introduced above.

The first theorem states that p-free parts of $\binom{n}{k}$ are uniformly distributed in residue classes modulo p^s and simultaneously spatially with respect to two--dimensional Lebesgue measure λ_2 (restricted to the triangle $\{(x,y) \in \mathbb{R}^2; 0 \le x \le y \le 1\}$ and normalised).

Theorem 1. *Let p be a prime, $s \ge 1$, and $(a,p) = 1$. Then for any λ_2-continuity set A we have*

$$\lim_{m\to\infty} \frac{2}{p^m(p^m+1)} \# \left\{ k,n\,;\, 0 \le k \le n < p^m \wedge \binom{n}{k}_{(p)} \equiv a \pmod{p^s} \wedge (k,n)p^{-m} \in A \right\} = \frac{\lambda_2(A)}{\phi(p^s)}. \tag{2}$$

Let μ be the $\frac{\log \frac{p(p+1)}{2}}{\log p}$-dimensional Hausdorff measure restricted to the "p-adic Sierpiński gasket"—the attractor of an iterated function system given in [13] and described below. The second theorem states that for given j the binomial coefficients with prescribed p-valuation equal to j exhibit a similar behaviour as well; their p-free parts are uniformly distributed modulo p^s, whereas they are spatially uniformly distributed with respect to μ.

Theorem 2. *Let p be a prime, $s \ge 1$, $j \ge 0$, and $(a,p) = 1$. Then for any μ-continuity set A we have*

$$\lim_{m\to\infty} \frac{\#\left\{k,n\,;\, 0 \le k \le n < p^m \wedge p^j \| \binom{n}{k} \wedge p^{-j}\binom{n}{k} \equiv a \pmod{p^s} \wedge (k,n)p^{-m} \in A\right\}}{\#\left\{0 \le k \le n < p^m\,;\, p^j \| \binom{n}{k}\right\}} = \frac{\mu(A)}{\phi(p^s)}. \tag{3}$$

Remark 1. Notice that Theorem 1 implies (1) choosing $A = \{(x,y)\,;\, 0 \le x \le y \le Np^{-\lfloor \log_p N \rfloor}\}$. Similarly, Theorem 2 implies [1, Theorem 6] (except for the error term) with the same choice of A.

2. Proofs

The proofs will make use of exponential sums involving additive characters on $\mathbb{R}^2$ and multiplicative characters on $\mathbb{Z}/p^s\mathbb{Z}$. As usual in this context, we write $e(t) = e^{2\pi i t}$.

In the sequel we will use the notation $(n!)_p$ for the product of all integers less than or equal to n, which are not divisible by p. Since the subscript p will only occur with factorials this should not cause any confusion. With the help of this notation we can formulate the following theorem due to A. Granville [7]. For an earlier version of this congruence we refer to [4].

Theorem 3. *Suppose that a prime power p^s and positive integers $n = m + r$ are given. Write $n = n_0 + n_1 p + \cdots + n_d p^d$ in base p, and let N_j be the least positive residue of $[n/p^j] \mod p^s$ for each $j \geq 0$ (so that $N_j = n_j + n_{j+1}p + \cdots \cdots + n_{j+s-1}p^{s-1}$); also make the corresponding definitions for m_j, M_j, r_j, R_j. Let e_j be the number of 'carries', when adding m and r in base p, on or beyond the jth digit. In particular, we have $p^{e_0} \| \binom{n}{m}$. Then*

$$\frac{1}{p^{e_0}}\binom{n}{m} \equiv (\pm 1)^{e_{s-1}} \left(\frac{(N_0!)_p}{(M_0!)_p (R_0!)_p}\right)\left(\frac{(N_1!)_p}{(M_1!)_p (R_1!)_p}\right)\cdots\left(\frac{(N_d!)_p}{(M_d!)_p (R_d!)_p}\right) \mod p^s, \tag{4}$$

where (± 1) is (-1) except if $p = 2$ and $s \geq 3$.

Preliminary results

We will make use of two technical Lemmas.

The first Lemma is [6, Lemma 5] (with 2 replaced by p).

Lemma 1. *Let $B(\mathbf{t})$ be a matrix function mapping vectors $\mathbf{t} \in \mathbb{R}^d$ to square matrices satisfying*

$$\|B(\mathbf{t}) - B\| \leq C\|\mathbf{t}\| \text{ for } \|\mathbf{t}\| \leq T, \tag{5}$$

$$|[B(\mathbf{t})]_{i,j}| \leq [B]_{i,j} \text{ for all } i, j \tag{6}$$

for some $C, T > 0$, some non-negative matrix B, and the matrix norm $\|\cdot\|$ induced by the maximum norm on the vector space. Assume that B has 1 as a simple dominating eigenvalue. Then the sequence of matrices

$$P_K(\mathbf{t}) = B\big(p^{-K}\mathbf{t}\big)B\big(p^{-(K-1)}\mathbf{t}\big)\cdots B\big(p^{-1}\mathbf{t}\big)$$

converges to a limit $P(\mathbf{t})$ for all $\mathbf{t}$; $P(\mathbf{t})$ is continuous at $\mathbf{t} = \mathbf{0}$.

In the sequel $\|\cdot\|$ will always denote the matrix norm induced by the maximum norm.

Remark 2. It is not stated in [6, Lemma 5] but immediately follows from the proof that if $B(\mathbf{t})$ depends continuously on $\mathbf{t}$, then the convergence to $P(\mathbf{t})$ as stated in the Lemma is uniform in $\mathbf{t}$ on compact subsets of $\mathbb{R}^d$ and $P(\mathbf{t})$ is continuous on $\mathbb{R}^d$. Furthermore, the relation $P(\mathbf{t}) = P(\mathbf{0})P(\mathbf{t})$ holds. Since the matrix $P(\mathbf{0})$ has rank 1 by the Perron-Frobenius theorem, this implies that the matrix $P(\mathbf{t})$ has rank at most 1.

The second lemma is a generalisation of Lemma 1.

Lemma 2. *Let $A(\mathbf{t})$ and $B(\mathbf{t})$ be matrix functions mapping vectors $\mathbf{t} \in \mathbb{R}^d$ continuously to square matrices satisfying*

$$\|B(\mathbf{t}) - B(\mathbf{0})\| \le C\|\mathbf{t}\| \qquad \text{for} \quad \|\mathbf{t}\| \le T, \tag{7}$$

$$\|A(\mathbf{t}) - A(\mathbf{0})\| \le C\|\mathbf{t}\| \qquad \text{for} \quad \|\mathbf{t}\| \le T, \tag{8}$$

$$|[B(\mathbf{t})]_{i,j}| \le [B(\mathbf{0})]_{i,j} \qquad \text{for} \quad i,j \text{ and all } \mathbf{t}, \tag{9}$$

$$|[A(\mathbf{t})]_{i,j}| \le [A(\mathbf{0})]_{i,j} \qquad \text{for} \quad i,j \text{ and all } \mathbf{t} \tag{10}$$

for some $C, T > 0$. Furthermore, assume that $B = B(\mathbf{0})$ has 1 as simple dominating eigenvalue and set $A = A(\mathbf{0})$. Define $P_K^{(j)}$ inductively by setting

$$P_K^{(0)}(\mathbf{t}) = B\big(p^{-K}\mathbf{t}\big)B\big(p^{-(K-1)}\mathbf{t}\big)\cdots B\big(p^{-1}\mathbf{t}\big),$$
$$P_0^{(0)}(\mathbf{t}) = I$$

and

$$P_K^{(j)}(\mathbf{t}) = \sum_{m=1}^{K} P_{K-m}^{(0)}(p^{-m}\mathbf{t})A(p^{-m}\mathbf{t})P_{m-1}^{(j-1)}(\mathbf{t}). \tag{11}$$

Then

$$P^{(j)}(\mathbf{t}) = \lim_{K\to\infty} \frac{P_K^{(j)}(\mathbf{t})}{\binom{K}{j}} = \big(P(\mathbf{0})A\big)^j P(\mathbf{t}), \tag{12}$$

where $P(\mathbf{t})$ is the limit given in Lemma 1. The convergence is uniform on compact subsets of $\mathbb{R}^d$.

Remark 3. Notice that $P_K^{(j)}(\mathbf{t})$ is the sum of all products of matrices $A(\cdot)$ and $B(\cdot)$ containing exactly j matrices $A(\cdot)$. In our application, this will reflect the combinatorial structure of j carries.

Proof. We proceed by induction on j to prove

$$\lim_{K\to\infty} \frac{P_K^{(j)}(\mathbf{t})}{\binom{K}{j}} = \big(P(\mathbf{0})A\big)P^{(j-1)}(\mathbf{t}).$$

From Lemma 1 and Remark 2 we have that $\big(P_K(\mathbf{t})\big)_K$ converges uniformly to $P(\mathbf{t})$ on compact subsets of $\mathbb{R}^d$, which is the case $j = 0$.

For the step $j-1 \to j$ we use the recursion formula (11). We split the range of summation into

$$m < \sqrt{K}, \quad \sqrt{K} \le m < K - \sqrt{K} \quad \text{and} \quad m \ge K - \sqrt{K}$$

and estimate the first and the last sum

$$\left\| \sum_{m<\sqrt{K}} P_{K-m}^{(0)}(p^{-m}\mathbf{t}) A(p^{-m}\mathbf{t}) P_{m-1}^{(j-1)}(\mathbf{t}) \right\| = \mathcal{O}\left(\sum_{m<\sqrt{K}} m^{j-1} \right) = \mathcal{O}(K^{j/2})$$

$$\left\| \sum_{K-\sqrt{K}\le m\le K} P_{K-m}^{(0)}(p^{-m}\mathbf{t}) A(p^{-m}\mathbf{t}) P_{m-1}^{(j-1)}(\mathbf{t}) \right\| = \mathcal{O}(K^{j-1}\sqrt{K}) = \mathcal{O}(K^{j-1/2}).$$

For the middle sum, we write

$$P_{K-m}(p^{-m}\mathbf{t}) = P(\mathbf{0}) + \mathrm{o}(1),$$
$$A(p^{-m}\mathbf{t}) = A + \mathrm{o}(1),$$

and

$$P_{m-1}^{(j-1)}(\mathbf{t}) = \binom{m-1}{j-1} P^{(j-1)}(\mathbf{t}) + \mathrm{o}(m^{j-1})$$

(which hold uniformly on compact subsets of $\mathbb{R}^d$) and insert these to obtain

$$\begin{aligned} &\sum_{\sqrt{K}\le m<K-\sqrt{K}} P_{K-m}^{(0)}(p^{-m}\mathbf{t}) A(p^{-m}\mathbf{t}) P_{m-1}^{(j-1)}(\mathbf{t}) \\ &= \sum_{\sqrt{K}\le m<K-\sqrt{K}} P(\mathbf{0}) A \binom{m-1}{j-1} P^{(j-1)}(\mathbf{t}) + \mathrm{o}(K^j) \\ &= \binom{K}{j} \big(P(\mathbf{0})A\big) P^{(j-1)}(\mathbf{t}) + \mathrm{o}(K^j). \end{aligned}$$

Putting everything together, we obtain (12). □

Proof of Theorem 1. We study the following exponential sum

$$S_\chi^{(1)}(m, t_1, t_2) = \sum_{0\le k\le n<p^m} \chi\left(\binom{n}{k}_{(p)} \right) e\left((kt_1 + nt_2)p^{-m} \right), \tag{13}$$

where χ denotes a Dirichlet character modulo p^s. In order to compute this sum, we construct a finite automaton, which computes $\binom{n}{k}$ modulo p^s with the help of (3).

Let $\mathcal{A} = \{0, 1, \dots, p-1\}^2$ be the alphabet. The set of states is given by

$$\mathcal{S} = \{0, \dots, p^{s-1} - 1\}^2 \times \{0, 1\}.$$

The transitions are defined by

$$(\varepsilon,\delta):(\nu,\kappa,\eta)\mapsto\begin{cases}\left(\lfloor\frac{\nu}{p}\rfloor+\varepsilon p^{s-2},\lfloor\frac{\kappa}{p}\rfloor+\delta p^{s-2},0\right) & \text{if } (\kappa \bmod p)+\eta\le\nu \bmod p,\\ \left(\lfloor\frac{\nu}{p}\rfloor+\varepsilon p^{s-2},\lfloor\frac{\kappa}{p}\rfloor+\delta p^{s-2},1\right) & \text{if } (\kappa \bmod p)+\eta>\nu \bmod p,\end{cases}\tag{14}$$

where $\kappa \bmod p$ denotes the non-negative remainder in the Euclidean division κ/p. The states $(\cdot,\cdot,0)$ represent the situation that no carry occurred in the subtraction of the least significant digits, whereas $(\cdot,\cdot,1)$ encode the situation that a carry occurred. A similar automaton was used in [13, 14] in the study of the p-adic Sierpiński gasket.

For a given pair of integers (n,k) we start at the state

$$\left(n \mod p^{s-1}, k \mod p^{s-1}\right);$$

technically, we would have to add extra states, which emulate reading the first $s-1$ digits.

For $\mathbf{t}=(t_1,t_2)\in\mathbb{R}^2$ we define the marked transition matrix $M_\chi(\mathbf{t})$ of the automaton defined above by

$$[M_\chi(\mathbf{t})]_{(\nu_1,\kappa_1,\eta_1),(\nu_2,\kappa_2,\eta_2)}=\begin{cases}\chi\Big((\pm1)^{\eta_1}\frac{(n!)_p}{(k!)_p((n-k-\eta_1)!)_p}\Big)e(\varepsilon t_1+\delta t_2) & \text{if } n-k-\eta_1\ge0\\ \qquad\text{and } \nu_2=\lfloor\frac{\nu_1}{p}\rfloor+\varepsilon p^{s-2} & \\ \qquad\text{and } \kappa_2=\lfloor\frac{\kappa_1}{p}\rfloor+\delta p^{s-2} & \\ \qquad\text{and } [\![(\kappa_1 \bmod p)+\eta_1>(\nu_1 \bmod p)]\!]=\eta_2, & \\ \chi\Big((\pm1)^{\eta_1}\frac{(n!)_p}{(k!)_p((p^{s-1}+n-k-\eta_1)!)_p}\Big)e(\varepsilon t_1+\delta t_2) & \text{if } n-k-\eta_1<0\\ \qquad\text{and } \nu_2=\lfloor\frac{\nu_1}{p}\rfloor+\varepsilon p^{s-2} & \\ \qquad\text{and } \kappa_2=\lfloor\frac{\kappa_1}{p}\rfloor+\delta p^{s-2} & \\ \qquad\text{and } [\![(\kappa_1 \bmod p)+\eta_1>(\nu_1 \bmod p)]\!]=\eta_2, & \\ 0, & \text{otherwise,}\end{cases}$$

where, for short, we denote

$$n=\nu_1+\varepsilon p^{s-1}\quad\text{and}\quad k=\kappa_1+\delta p^{s-1}.$$

The value (±1) is chosen according to Theorem 3. Here and later on we use Iverson's notation $[\![A]\!]$, which is 1, if A is true, and 0 otherwise.

Then we have

$$S_\chi^{(1)}(m,\mathbf{t})=\mathbf{v}(p^{-m}\mathbf{t})^T M_\chi\big(p^{-(m-s)}\mathbf{t}\big)M_\chi\big(p^{-(m-s-1)}\mathbf{t}\big)\cdots M_\chi(p^{-1}\mathbf{t})\mathbf{w},\tag{15}$$

where $\mathbf{w}$ denotes the column vector with all entries $(1-\eta)$.

The vector $\mathbf{v}(\mathbf{t})$ is given by

$$[\mathbf{v}(\mathbf{t})]_{(\nu,\kappa,\eta)} = e\big((\nu t_1 + \kappa t_2)\big).$$

We write $\mathbf{1}$ for the vector with all entries 1 and observe that $\mathbf{v}(\mathbf{0}) = \mathbf{1}$.

We notice that the automaton defined by the transition function (14) has exactly p^2 transitions emanating from each state. The marked transition matrix $M_{\chi_0}(\mathbf{0})$ (χ_0 being the principal character) marks each of these transitions by 1; thus this matrix has exactly p^2 entries 1 per line and is a Perron-Frobenius matrix with dominating eigenvalue p^2. From (13) the sum $S_\chi^{(1)}(m,\mathbf{t})$ has $\frac{p^m(p^m+1)}{2}$ summands. Thus we divide (15) by $\frac{p^m(p^m+1)}{2}$ and let m tend to infinity. For the principal character this results in

$$\hat\lambda(\mathbf{t}) = \lim_{m\to\infty}\left(\frac{p^m(p^m+1)}{2}\right)^{-1} S_{\chi_0}(m,\mathbf{t}) = \mathbf{1}^T P(\mathbf{t})\mathbf{w}, \tag{16}$$

where

$$P(\mathbf{t}) = \lim_{m\to\infty}\left(\frac{p^m(p^m+1)}{2}\right)^{-1} M_{\chi_0}\big(p^{-(m-s)}\mathbf{t}\big) M_{\chi_0}\big(p^{-(m-s-1)}\mathbf{t}\big)\cdots M_{\chi_0}(p^{-1}\mathbf{t})$$

is a convergent infinite matrix product applying Lemma 1 with $B(\mathbf{t}) = \frac{1}{p^2} M_{\chi_0}(\mathbf{t})$.

The limit $\hat\lambda(\mathbf{t})$ is the Fourier transform of the two-dimensional Lebesgue measure restricted to the triangle $\{(x,y)\in\mathbb{R}^2\,;\,0\le x\le y\le 1\}$, normalised to total measure 1.

For non-principal characters χ, at least one non-zero entry of $M_\chi(\mathbf{0})$ differs from 1, because $\binom{n}{1}_{(p)} = n_{(p)}$ implies that the character is evaluated at all prime residue classes $(\mathrm{mod}\ p^s)$; thus we have

$$\|M_\chi(\mathbf{0})\| < p^2.$$

From this we conclude, using the continuity of $M_\chi(\mathbf{t})$ at $\mathbf{t}=\mathbf{0}$,

$$\lim_{m\to\infty}\left(\frac{p^m(p^m+1)}{2}\right)^{-1} S_\chi(m,\mathbf{t})$$

$$= \mathbf{1}^T \lim_{m\to\infty}\left(\frac{p^m(p^m+1)}{2}\right)^{-1} M_\chi\big(p^{-(m-s)}\mathbf{t}\big) M_\chi\big(p^{-(m-s-1)}\mathbf{t}\big)\cdots M_\chi(p^{-1}\mathbf{t})\mathbf{w} = 0.$$

Summing up, we have

$$\lim_{m\to\infty}\left(\frac{p^m(p^m+1)}{2}\right)^{-1} \sum_{0\le k\le n<p^m} \left[\!\!\left[\binom{n}{k}_{(p)} \equiv a \pmod{p^s}\right]\!\!\right] e\big((nt_1+kt_2)p^{-m}\big)$$

$$= \frac{1}{\phi(p^s)}\sum_\chi \overline{\chi(a)} \lim_{m\to\infty}\left(\frac{p^m(p^m+1)}{2}\right)^{-1} S_\chi^{(1)}(m,\mathbf{t}) = \frac{1}{\phi(p^s)}\hat\lambda(\mathbf{t}),$$

which finishes the proof of Theorem 1 by Levy's continuity theorem. □

P r o o f o f T h e o r e m 2. In order to obtain the desired result, we study the exponential sum

$$S_\chi^{(2)}(m,j,t_1,t_2)=\sum_{0\le k\le n<p^m}\left[\!\left[p^j\|\binom{n}{k}\right]\!\right]\chi\left(p^{-j}\binom{n}{k}\right)e\big((kt_1+nt_2)p^{-m}\big). \quad (17)$$

The underlying automaton is the same as in the proof of Theorem 1, but we have to take into account the number of carries in the subtraction. This is done by a new marking of the transitions using the following two matrices

$$[B(\mathbf{t})]_{(\nu_1,\kappa_1,\eta_1),(\nu_2,\kappa_2,\eta_2)}=\begin{cases}\frac{2}{p(p+1)}[M_{\chi_0}(\mathbf{t})]_{(\nu_1,\kappa_1,\eta_1),(\nu_2,\kappa_2,\eta_2)} & \text{if } \eta_1=0,\\ 0 & \text{if } \eta_1=1,\end{cases}$$

$$[A(\mathbf{t})]_{(\nu_1,\kappa_1,\eta_1),(\nu_2,\kappa_2,\eta_2)}=\begin{cases}[M_{\chi_0}(\mathbf{t})]_{(\nu_1,\kappa_1,\eta_1),(\nu_2,\kappa_2,\eta_2)} & \text{if } \eta_1=1,\\ 0 & \text{if } \eta_1=0.\end{cases}$$

The matrix $B(\mathbf{t})$ encodes all transitions without carry, whereas $A(\mathbf{t})$ encodes a carry in the subtraction of the least significant digit. Notice that we normalise $B(\mathbf{t})$ to satisfy the assumption of Lemma 2.

We obtain

$$S_{\chi_0}(m,j,\mathbf{t})=\left(\frac{p(p+1)}{2}\right)^m\sum_{\ell=0}^{\min(j,s-1)}\mathbf{v}_\ell(p^{-m}\mathbf{t})^TP_{m-s}^{(j-\ell)}(\mathbf{t})\mathbf{w}, \quad (18)$$

where the vectors $\mathbf{v}_\ell$ encode starting blocks of $s-1$ digits containing ℓ carries in the subtraction:

$$\mathbf{v}_\ell(\mathbf{t})_{(\nu,\kappa,\eta)}=\begin{cases}e(\nu t_1+\kappa t_2) & \text{if } \eta=[\![\nu<\kappa]\!] \text{ and there are exactly } \ell \text{ carries}\\ & \text{in the subtraction } \eta p^s+\nu-\kappa,\\ 0, & \text{otherwise.}\end{cases}$$

Applying Lemma 2 yields

$$\lim_{m\to\infty}\frac{S_{\chi_0}(m,j,\mathbf{t})}{\binom{m}{j}\left(\frac{p(p+1)}{2}\right)^m}=\mathbf{v}_0(\mathbf{0})^T\big(P(\mathbf{0})A\big)^jP(\mathbf{t})\mathbf{w}. \quad (19)$$

We now observe that $\mathbf{v}_0(\mathbf{0})$ is a vector with non-negative entries and $(P(\mathbf{0})A)^j$ is a matrix with non-negative entries. Thus $\mathbf{v}_0(\mathbf{0})^T\big(P(\mathbf{0})A\big)^j$ is a vector with non-negative entries. Using the relation $P(\mathbf{t})=P(\mathbf{0})P(\mathbf{t})$, we can rewrite the limit (19) as

$$\mathbf{v}_0(\mathbf{0})^T\big(P(\mathbf{0})A\big)^jP(\mathbf{0})P(\mathbf{t})\mathbf{w};$$

the vector $\mathbf{v}_0(\mathbf{0})^T\big(P(\mathbf{0})A\big)^jP(\mathbf{0})$ is now proportional to the left Perron-Frobenius eigenvalue of B, because $P(\mathbf{0})$ is a matrix of rank 1 with this eigenvector. Thus the limit (19) is proportional to $\mathbf{v}^TP(\mathbf{t})\mathbf{w}$ for any non-negative vector $\mathbf{v}$.

We set

$$\hat{\mu}(\mathbf{t}) = \lim_{m\to\infty} \frac{S_{\chi_0}(m,0,\mathbf{t})}{\left(\frac{p(p+1)}{2}\right)^m}.$$

Then by the above argument, we have

$$\hat{\mu}(\mathbf{t}) = \lim_{m\to\infty} \frac{S_{\chi_0}(m,j,\mathbf{t})}{S_{\chi_0}(m,j,\mathbf{0})}.$$

From [13] we infer that the sets

$$Q_m = \left\{(n,k)p^{-m}\,;\, 0 \le k \le n < p^m \text{ and } p \not| \binom{n}{k}\right\}$$

tend to the attractor Q of the iterated function system defined by

$$F_{a,b}(x,y) = \left(\frac{x+a}{p}, \frac{y+b}{p}\right),$$

where $0 \le b \le a < p$ (the "p-adic Sierpiński triangle").

Furthermore, the measures

$$\mu_m = \frac{1}{\left(\frac{p(p+1)}{2}\right)^m} \sum_{\mathbf{x}\in Q_m} \delta_{\mathbf{x}}$$

tend to the Hausdorff measure of dimension $s = \frac{\log \frac{p(p+1)}{2}}{\log p}$ restricted to Q and normalised to total mass 1. This implies that $\hat{\mu}(\mathbf{t})$ is the Fourier transform of this measure.

In order to sieve out the binomial coefficients with $p^{-j}\binom{n}{k} \equiv a \pmod{p^s}$ we consider the sum

$$\frac{1}{\phi(p^s)} \sum_{\chi} \overline{\chi(a)} S_{\chi}(m,j,\mathbf{t})$$

and observe, using the same arguments as in the proof of Theorem 1, that $S_{\chi}(m,j,\mathbf{t})$ (for $\chi \neq \chi_0$) is of smaller order of magnitude than $S_{\chi_0}(m,j,\mathbf{t})$. This finishes the proof of Theorem 2. □

REFERENCES

[1] BARAT, G.—GRABNER, P. J.: *Digital functions and distribution of binomial coefficients*, J. London Math. Soc. **64** (2001), 523–547.

[2] BARBOLOSI, D.—GRABNER, P. J.: *Distribution des coefficients multinomiaux et q-binomiaux modulo p*, Indag. Math. **7** (1996), 129–135.

[3] CARLITZ, L.: *The number of binomial coefficients divisible by a fixed power of a prime*, Rend. Circ. Matem. Palermo **16** (1967), 299–320.

[4] DAVIS, K. S.—WEBB, W.: *Lucas congruence for prime powers*, European J. Combin. **11** (1990), 229–233.
[5] GARFIELD, R.—WILF, H. S.: *The distribution of the binomial coefficients modulo p*, J. Number Theory **41** (1992), 1–5.
[6] GRABNER, P. J.—HEUBERGER, C.—PRODINGER, H.: *Counting optimal joint digit expansions*, Integers **5** (2005), no. 3, A09, 19 pages (electronic).
[7] GRANVILLE, A.: *Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers*, Organic mathematics (Burnaby, BC, 1995), Amer. Math. Soc., Providence, RI, 1997, pp. 253–276.
[8] GREINECKER, F.: *Spatial equidistribution of combinatorial number schemes*, J. Fractal Geom. (2016) (to appear).
[9] KUMMER, E. E.: *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*, J. reine angew. Math. **44** (1852), 93–146.
[10] LUCAS, É: *Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques, suivant un module premier*, Bull. Soc. Math. France **6** (1878), 49–54.
[11] SINGMASTER, D.: *Notes on binomial coefficients, I—A generalization of Lucas' congruence, II—The least n such that p^e divides an r-nomial coefficient of rank n, III—Any integer divides almost all binomial coefficients*, J. London Math. Soc. **8** (1974), 545–548, 549–554, 555–560.
[12] SPIEGELHOFER, L.—WALLNER, M.: *Divisibility of binomial coefficients by powers of primes*, arXiv:1604.07089, 2016.
[13] VON HAESELER, F.—PEITGEN, H.-O.—SKORDEV, G.: *Pascal's triangle, dynamical systems and attractors*, Ergodic Theory Dynam. Systems **12** (1992), no. 3, 479–486.
[14] ———, *Cellular automata, matrix substitutions and fractals*, Ann. Math. Artificial Intelligence **8** (1993), 345–362. (Theorem proving and logic programming (1992).)

Received May 10, 2016
Accepted June 14, 2016

Guy Barat
Peter J. Grabner
Institut für Analysis und Zahlentheorie
Technische Universität Graz
Kopernikusgasse 24
8010 Graz
AUSTRIA
E-mail: guy.barat@tugraz.at
peter.grabner@tugraz.at