ACTA ARITHMETICA
LXXXIV.1 (1998)

On some arithmetical properties of middle binomial coefficients

by

Daniel Berend (Beer-Sheva)
and Jørgen E. Harmse (Austin, Tex.)

1. Introduction and main results. Arithmetical properties of binomial coefficients have been studied by many authors. Of particular interest is the sequence of middle binomial coefficients $\binom{2n}{n}$. Perhaps some of this interest is due to its historic role in the proof of the prime number theorem. For example, Erdős conjectured that $\binom{2n}{n}$ is not square-free for every $n > 4$ (see, for example, [EG]). This conjecture has been recently settled affirmatively by Granville and Ramaré [GR] and Velammal [V] (and formerly, for sufficiently large n, by Sárközy [Sár]; see also [San] and [EK]). Another relevant result is that no middle binomial coefficient can be written in a non-trivial way as a product of other such coefficients [E].

In this paper we discuss the behaviour of the sequence modulo prime powers. Our first result is

Theorem 1.1. *For every odd prime power p^e and congruence class $p^e\mathbb{Z}+s$, there exist infinitely many positive integers n such that $\binom{2n}{n} \in p^e\mathbb{Z}+s$.*

The theorem may be rephrased as the assertion that the sequence $\left(\binom{2n}{n}\right)_{n=1}^{\infty}$, considered as a sequence in the ring of p-adic integers, is dense in that ring.

Remark 1.1. The assertion of Theorem 1.1 fails modulo powers of 2 since $\binom{2n}{n}$ is even for all $n \geq 1$.

Next, it is natural to ask how the sequence $\binom{2n}{n}$ is distributed modulo p^e, namely with what asymptotic proportion it assumes each of the p^e possible values. A few trials (or a knowledge of a certain classical fact regarding

1991 *Mathematics Subject Classification*: Primary 11B50, 11B65, 05A10, 11K99; Secondary 11T99.

Research of the first author supported in part by the Israel Science Ministry, the Basic Research Foundation and the Bi-National Israel–USA Science Foundation.

binomial coefficients, to be formulated subsequently as Theorem 2.1) may convince one that the sequence is nearly always 0 modulo p^e even though, according to Theorem 1.1, each of the other $p^e - 1$ values is also assumed infinitely often. Thus it makes sense to compare the relative frequencies of the non-zero classes modulo p^e. By the same token, the classes of the form $p^e\mathbb{Z}+sp^{e-1}$, $1 \le s \le p-1$, appear much more frequently than the others. In general, one may expect $\binom{2n}{n}$ to belong to two classes $p^e\mathbb{Z}+s_1$ and $p^e\mathbb{Z}+s_2$ with the same asymptotic frequency if and only if the exact power of p dividing s_1 and s_2 is the same. Our next theorem, to be stated after a few definitions, is a weaker version of this.

A sequence of integers $(a_n)_{n=1}^{\infty}$ is *uniformly distributed* ([KN, p. 305], [N, p. 1]) modulo a positive integer l if

$$\frac{\#(\{1 \le n \le N : a_n \equiv s \pmod{l}\})}{N} \xrightarrow[N\to\infty]{} \frac{1}{l}, \qquad s = 0, 1, \ldots, l-1,$$

where $\#(F)$ denotes the cardinality of a finite set F. The sequence is *weakly uniformly distributed* modulo l [N, p. 8] (see also [KN, p. 318] and the references listed there) if $(a_n, l) = 1$ infinitely often and

$$\frac{\#(\{1 \le n \le N : a_n \equiv s \pmod{l}\})}{\#(\{1 \le n \le N : (a_n, l) = 1\})} \xrightarrow[N\to\infty]{} \frac{1}{\phi(l)}, \qquad s = 1, \ldots, l-1,\ (s, l) = 1.$$

Now, in general, the notion of uniform distribution has a stronger version where instead of requiring only that the dispersion of large initial pieces of the sequence becomes more and more even, we require this to happen for any large finite portion of the sequence. This version is termed *well-distribution* [KN, pp. 84, 200, 221]. We are specifically interested in the following

Definition 1.1. The sequence $(a_n)_{n=1}^{\infty}$ is *weakly well-distributed* modulo l if $(a_n, l) = 1$ infinitely often and

$$\frac{\#(\{M \le n \le N : a_n \equiv s \pmod{l}\})}{\#(\{M \le n \le N : (a_n, l) = 1\})} \xrightarrow[N-M\to\infty]{} \frac{1}{\phi(l)},$$
$$s = 1, \ldots, l-1,\ (s, l) = 1.$$

Theorem 1.2. *For every odd prime p, the sequence $\left(\binom{2n}{n}\right)_{n=1}^{\infty}$ is weakly well-distributed modulo p.*

Remark 1.2. As mentioned earlier, one may actually expect the theorem to be true modulo p^e. Unfortunately, this stronger result does not follow from our method. The problem lies with the complicated formula for calculating binomial coefficients modulo a prime power versus the simple formula in case of a prime (see Theorems 2.1 and 2.2 *infra*).

It is of interest to mention here results in a similar spirit, by Hexel [Hex], Hexel and Sachs [HS], and Garfield and Wilf [GW]. They considered the number of entries in each row of Pascal's triangle belonging to each of the residue classes modulo p, and were able to calculate the generating function. Another closely related work is due to Barbolosi and Grabner [BG], who considered the number of entries in the first n rows of Pascal's triangle, assuming each value modulo p. It follows from their results in particular that each of the non-zero values appears with the same asymptotic frequency.

Theorem 1.2 will be proved using a rather more general result. To state this, we recall a few additional definitions. A sequence $(a_n)_{n=1}^{\infty}$ in a compact group G is *uniformly distributed* if it is uniformly distributed with respect to the Haar measure μ on G, namely if

$$\frac{1}{N}\sum_{n=1}^{N} f(a_n) \xrightarrow[N\to\infty]{} \int_G f\,d\mu$$

for every continuous real-valued function f on G [KN, p. 221]. The generalization of the concept of well-distribution is obvious. (Thus, the above definitions referred to the case where G is the additive group of the ring $\mathbb{Z}/l\mathbb{Z}$, or, alternatively, after discarding those terms of our sequence which are not relatively prime to l, the multiplicative group of the same ring.)

Theorem 1.3. *Let G be a compact group and $\alpha_0, \alpha_1, \ldots, \alpha_{r-1} \in G$. Consider the sequence $(a_n)_{n=1}^{\infty}$ defined as follows: If $n = d_0 + d_1 r + \ldots + d_k r^k$ is the base r expansion of n ($0 \le d_i \le r-1$ with $d_k > 0$ for $n > 0$), then*

$$a_n = \alpha_{d_0}\alpha_{d_1}\ldots\alpha_{d_k}.$$

Assume that:

(1) *The closed subgroup of G generated by $\alpha_0, \alpha_1, \ldots, \alpha_{r-1}$ is G itself.*

(2) *No coset of a proper closed normal subgroup of G contains all the elements $\alpha_0, \alpha_1, \ldots, \alpha_{r-1}$.*

Then $(a_n)_{n=1}^{\infty}$ is well-distributed in G.

For the proofs we shall require a few results concerning congruences of various binomial coefficients and other quantities. These results seem to be of independent interest, and are stated separately in Section 2. All proofs are carried out in Section 3. In Section 4 we present a result of Erdős, Graham, Ruzsa and Straus [EGRS], relating to the behaviour of the middle binomial coefficients modulo products of two distinct primes.

We would like to express our gratitude to J. P. Allouche, Y. Bilu, Y. Caro and M. Lin for their helpful comments on an earlier draft of this paper. We thank also the referee for the numerous points he raised, which added to the presentation of the paper.

2. Some congruences.

We start with a few known results concerning the values of certain binomial coefficients modulo prime powers.

Theorem 2.1 [L, Sec. XXI]. *Let m and n be non-negative integers with base p expansions*

$$n=\sum_{i=0}^{k} n_i p^i, \qquad m=\sum_{i=0}^{k} m_i p^i, \qquad (0\le n_i, m_i < p).$$

(1) *If $m_i > n_i$ for some i, then $p \mid \binom{n}{m}$.*

(2) *If $m_i \le n_i$ for each i, then*

$$\binom{n}{m} \equiv \prod_{i=0}^{k}\binom{n_i}{m_i} \pmod{p}. \tag{2.1}$$

Note that, putting $\binom{a}{b}=0$ for $a<b$, we may view the first part of the theorem as a special case of the second. Also, there is a simple formula for the exact power of p dividing $\binom{n}{m}$. Namely, let e be the number of carries when adding m and $n-m$ as numbers written in base p. Then $p^e \mid \binom{n}{m}$ but $p^{e+1} \nmid \binom{n}{m}$ [K, pp. 115f].

A result which gives readily an extension of (2.1) to prime power moduli is the following one, due to Granville.

Theorem 2.2 [Gran]. *If p does not divide $\binom{n}{m}$, then*

$$\binom{n}{m} \equiv \binom{[n/p]}{[m/p]}\binom{n'}{m'}\Big/\binom{[n'/p]}{[m'/p]} \pmod{p^e},$$

where l' denotes the least non-negative residue of an integer l modulo p^e.

Iterating this formula we find that, if p does not divide $\binom{n}{m}$, then, denoting

$$P=\prod_{i=0}^{k-e+1}\binom{n_i+n_{i+1}p+\ldots+n_{i+e-1}p^{e-1}}{m_i+m_{i+1}p+\ldots+m_{i+e-1}p^{e-1}}$$

and

$$Q=\prod_{i=1}^{k-e+1}\binom{n_i+n_{i+1}p+\ldots+n_{i+e-2}p^{e-2}}{m_i+m_{i+1}p+\ldots+m_{i+e-2}p^{e-2}},$$

we have

$$\binom{n}{m} \equiv \frac{P}{Q} \pmod{p^e}. \tag{2.2}$$

Proposition 2.1. *For any prime p and positive integers a, e*

$$\binom{2ap^e}{ap^e} \equiv \binom{2ap^{e-1}}{ap^{e-1}} \begin{cases} \pmod{4}, & p=2,\ e=1,\\ \pmod{2^{3e}}, & p=2,\ e>1,\\ \pmod{3^{3e-1}}, & p=3,\\ \pmod{p^{3e}}, & p\ge 5.\end{cases}$$

Remark 2.1. This proposition, as well as the next one, are generalizations of known results. Our proofs, in the next section, follow those given by Gardiner [Ga], with slight modifications for the more general case.

Remark 2.2. It follows from the proposition, in particular, that for any prime p and positive integer a the sequence $\left(\binom{2ap^e}{ap^e}\right)_{e=1}^{\infty}$, considered as a sequence in the ring $\mathbb{Z}_p$ of p-adic integers, is convergent. While this is of no direct bearing upon the paper, it would be interesting to know whether the limit is some "recognizable" number.

We shall use the convention that $\sum'$ denotes sums taken only over those elements in the index set which are relatively prime to the relevant modulus p.

Proposition 2.2. *For every prime p and positive integers a, e,*

(1)

$$\sum_{j=1}^{ap^e}{}' \frac{1}{j} \equiv 0 \begin{cases} (\text{mod } 2^{2e-2}), & p=2,\ e>1, \\ (\text{mod } 3^{2e-1}), & p=3, \\ (\text{mod } p^{2e}), & p\ge 5. \end{cases} \tag{2.3}$$

(2)

$$\sum_{j=1}^{ap^e}{}' \frac{1}{j^2} \equiv 0 \begin{cases} (\text{mod } 2^{e-1}), & p=2,\ e>1, \\ (\text{mod } 3^{e-1}), & p=3,\ e>1, \\ (\text{mod } p^{e}), & p\ge 5. \end{cases} \tag{2.4}$$

(3)

$$\sum_{1\le j<k\le ap^e}{}' \frac{1}{jk} \equiv 0 \begin{cases} (\text{mod } 2^{e-2}), & p=2,\ e>2, \\ (\text{mod } 3^{e-1}), & p=3, \\ (\text{mod } p^{e}), & p\ge 5. \end{cases} \tag{2.5}$$

3. Proofs

Proof of Proposition 2.2. (2) Since inversion is a 1-1 map on the group of units $(\mathbb{Z}/p^e\mathbb{Z})^\times$ of the ring $\mathbb{Z}/p^e\mathbb{Z}$, we have

$$\begin{aligned}\sum_{j=1}^{ap^e}{}' \frac{1}{j^2} &\equiv a\sum_{j=1}^{p^e}{}' \frac{1}{j^2} \equiv a\sum_{j=1}^{p^e}{}' j^2 = a\Big(\sum_{j=1}^{p^e} j^2 - \sum_{j=1}^{p^{e-1}} (pj)^2\Big) \\ &= \frac{a}{6}[p^e(p^e+1)(2p^e+1) - p^{e+1}(p^{e-1}+1)(2p^{e-1}+1)].\end{aligned}$$

Now the expression inside the brackets is clearly divisible by p^e. As the initial factor of $1/6$ reduces the exponent by 1 for $p=2,3$, we arrive at (2.4).

(1) We have

$$\sum_{j=1}^{ap^e}{}' \frac{1}{j} = \frac{1}{2}\sum_{j=1}^{ap^e}{}' \left(\frac{1}{j} + \frac{1}{ap^e - j}\right) = \frac{ap^e}{2}\sum_{j=1}^{ap^e}{}' \frac{1}{j(ap^e - j)}.$$

Now

$$\sum_{j=1}^{ap^e}{}' \frac{1}{j(ap^e - j)} \equiv \sum_{j=1}^{ap^e}{}' \frac{-1}{j^2} \pmod{p^e},$$

so that, along with (2.4), we obtain (2.3).

(3) We have

$$\sum_{1\le j<k\le ap^e}{}' \frac{1}{jk} = \frac{1}{2}\left[\left(\sum_{j=1}^{ap^e}{}' \frac{1}{j}\right)^2 - \sum_{j=1}^{ap^e}{}' \frac{1}{j^2}\right],$$

which implies (2.5).

Proof of Proposition 2.1. For $p = 2,\ e = 1$, we have

$$\binom{4a}{2a} = \prod_{j=1}^{2a} \frac{2a + j}{j} = \prod_{k=1}^{a} \frac{2a + 2k}{2k} \prod_{j=1}^{2a}{}' \left(1 + 2\frac{a}{j}\right) = \binom{2a}{a}(1 + 2S),$$

where S is a rational which is a 2-adic integer. Since $\binom{2a}{a}$ is even, we obtain $\binom{4a}{2a} \equiv \binom{2a}{a} \pmod 4$. In all other cases we have

$$\begin{aligned}\binom{2ap^e}{ap^e} &= \prod_{j=1}^{ap^e} \frac{ap^e + j}{j} = \prod_{k=1}^{ap^{e-1}} \frac{ap^e + kp}{kp} \prod_{j=1}^{ap^e}{}' \frac{2ap^e - j}{j} \\ &= \binom{2ap^{e-1}}{ap^{e-1}} \prod_{j=1}^{ap^e}{}' \left(-1 + 2ap^e \cdot \frac{1}{j}\right) \\ &= \binom{2ap^{e-1}}{ap^{e-1}} \cdot \left[1 - 2ap^e \sum_{j=1}^{ap^e}{}' \frac{1}{j} + 4a^2p^{2e} \sum_{1\le j<k\le ap^e}{}' \frac{1}{jk} + p^{3e}S\right],\end{aligned}$$

where S is a p-adic integer. In view of Proposition 2.2, this completes the proof.

Proof of Theorem 1.1. We first consider the case $e = 1$, $(s,p) = 1$. In view of Theorem 2.1, when trying to find suitable integers n, we have to make sure that all digits in their base p expansion are $\le (p-1)/2$. From (2.1) it follows that the set R of all residue classes s relatively prime to p appearing infinitely often forms a multiplicative subsemigroup, and therefore subgroup, of $(\mathbb{Z}/p\mathbb{Z})^\times$. Moreover, the residue classes of all the numbers $\binom{2g}{g}$,

$1 \le g \le (p-1)/2$, belong to R. In particular, the residue class of $\binom{2}{1} = 2$ belongs to R. Now

$$2^{-1}\binom{2g}{g}\Big/\binom{2(g-1)}{g-1} = \frac{2g(2g-1)}{2g^2} = \frac{2g-1}{g},$$

which implies that for $g \in \{2,3,4,\ldots,(p-1)/2\}$ the residue class of $(2g-1)/g$ is in R. Suppose that R is a proper subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$, and let k be the least positive integer whose residue class is not in R. Then k is odd (since $2 \in R$) and $2 \le k \le p-1$, so $k = 2g-1$ for some $g \in \{2,3,4,\ldots,(p-1)/2\}$. Now $g < k$ so the residue classes of $(2g-1)/g$ and g are in R, so the residue class of $k = g \cdot (2g-1)/g$ is in R. Since this is a contradiction, $R = (\mathbb{Z}/p\mathbb{Z})^\times$, which concludes this case.

Now let us consider the case $e = 2$, $(s,p) = 1$. From Proposition 2.1 it follows in particular that

$$\binom{2ap}{ap} \equiv \binom{2a}{a} \pmod{p^2}, \qquad a = 1,2,\ldots,(p-1)/2.$$

Consider the value of $\binom{2n}{n}$ only for numbers n of the form $n = n_0 + n_1p^2 + \ldots + n_kp^{2k}$ with $0 \le n_i \le (p-1)/2$ for each i (the important point here being that the base p expansion of n contains no two consecutive non-zero digits). From (2.2) and Proposition 2.1 it follows that for such n,

$$\binom{2n}{n} \equiv \prod_{i=0}^{k}\binom{2n_ip}{n_ip} \pmod{p^2}.$$

Let R be the set of residue classes modulo p^2 appearing infinitely often among these values. Then R is a subgroup of $(\mathbb{Z}/p^2\mathbb{Z})^\times$ and contains the residue classes of all numbers of the form $\binom{2g}{g}$, where $1 \le g \le (p-1)/2$. As in the preceding case, the residue classes of $1,2,\ldots,p-1$ are in R. Moreover, $-1 \equiv p^2 - 1 = 2 \cdot \frac{p+1}{2} \cdot (p-1)$, so the residue classes of $-1,-2,\ldots,-(p-1)$ are in R. Consider s as an element of $(\mathbb{Z}/p^2\mathbb{Z})^\times$. Suppose $s \notin R$. Then $s, 2s, \ldots, (p-1)s \notin R$. Moreover, writing $(\mathbb{Z}/p^2\mathbb{Z})^\times = \bigcup_{i=0}^{p-1} C_i$, where C_i consists of the residue classes of $ip+1, ip+2, \ldots, ip+p-1$, we see that none of those multiples of s belongs to either C_0 or C_{p-1}. Hence for some $1 \le t_1 < t_2 \le p-1$ and $1 \le i \le p-2$ we have $t_1s, t_2s \in C_i$, so that $(t_2-t_1)s \in C_0 \cup C_{p-1}$, which is a contradiction. Consequently, $R = (\mathbb{Z}/p^2\mathbb{Z})^\times$, which concludes this case.

Next we turn to the case of general e, still with $(s,p) = 1$. In view of the preceding case, we can find some $n_0 \in \mathbb{N}$ such that $\binom{2n_0}{n_0}$ is a primitive root modulo p^2, and therefore a primitive root modulo p^e. Examining the proof in the preceding case we notice that n_0 may be assumed to contain arbitrarily many zeros (e zeros is what we need) between any two non-zero digits in its base p expansion. Take a $u \in \mathbb{N}$ such that $\binom{2n_0}{n_0}^u \equiv s$

(mod p^e). Construct a positive integer n by concatenating u times the base p expansion of n_0, again leaving blocks of e consecutive zeros between any two occurrences of the block corresponding to n_0 (i.e., $n = \sum_{j=0}^{u-1} p^{j(e+d)} n_0$, where $d = 1 + \lfloor \log_p n_0 \rfloor$). Again using (2.2) we obtain $\binom{2n}{n} \equiv \binom{2n_0}{n_0}^u \equiv s$ (mod p^e). As the condition on u determines it only modulo $\phi(p^e)$, we again find infinitely many solutions for our equation.

Arriving finally at the general case, we may assume that $s = cp^k$, where $1 \le c < p^{e-k}$, $(c,p) = 1$ and $1 \le k < e$. Without loss of generality we may assume that $e > 2k$. A slight modification of the discussion in the former case shows that there exist infinitely many numbers n such that $n \equiv p^k$ (mod p^e) and $\binom{2n}{n} \equiv c(4p^k - 2) \pmod{p^{e-k}}$. For such n we have

$$\binom{2(n-1)}{n-1} = \frac{n}{4n-2}\binom{2n}{n} \equiv cp^k \pmod{p^e}.$$

Hence our equation has again infinitely many solutions, which completes the proof.

We now turn to the proof of Theorem 1.3. One way to tackle it is by trying to prove that the sequence of measures defined by

$$\mu_N = \frac{1}{N}\sum_{n=0}^{N-1} \delta_{a_n}, \qquad N = 0, 1, 2, \ldots$$

converges weakly to the Haar measure on G, where δ_x denotes the Dirac measure supported at x. (Of course, this would prove only uniform distribution. For well-distribution one needs to let the index range over arbitrary long intervals.) It turns out that, in case $\alpha_0 = 1$, the measure μ_{r^n} is the n-fold convolution of μ_r. Hence, using Ito–Kawada's theorem (cf. [Hey] or [R]) one can proceed to show the required convergence holds at least for the subsequence of measures μ_{r^n}. Our approach is basically equivalent, but is more direct, and hence more likely to be applicable, say, to obtaining discrepancy estimates.

LEMMA 3.1. *Under the assumptions of Theorem* 1.3, *for every irreducible unitary representation* $\sigma \ne 1$ *of* G *we have*

$$\frac{1}{r^n}(\sigma(\alpha_0) + \sigma(\alpha_1) + \ldots + \sigma(\alpha_{r-1}))^n \xrightarrow[n\to\infty]{} 0.$$

Proof. It suffices to prove that all eigenvalues of the matrix

$$\frac{\sigma(\alpha_0) + \sigma(\alpha_1) + \ldots + \sigma(\alpha_{r-1})}{r}$$

are strictly less than 1 in their absolute value. Since for every vector v we have

$$\left\|\frac{\sigma(\alpha_0)+\sigma(\alpha_1)+\ldots+\sigma(\alpha_{r-1})}{r}v\right\| \le \frac{1}{r}\sum_{i=0}^{r-1}\|\sigma(\alpha_i)v\| = \|v\|, \tag{3.1}$$

all those eigenvalues are of absolute value not exceeding 1. Suppose λ is an eigenvalue with $|\lambda| = 1$. If v is an eigenvector corresponding to the eigenvalue λ, then, by (3.1),

$$\sigma(\alpha_i)v = \lambda v, \qquad i = 0, 1, \ldots, r-1.$$

It follows that v is a common eigenvector of the matrices $\sigma(\alpha_i)$, $i = 0, 1, \ldots, r-1$, and hence an eigenvector of $\sigma(x)$ for every x in the subgroup generated by the α_i's. Since this subgroup is dense in G, it follows that v is an eigenvector of $\sigma(x)$ for every $x \in G$. As σ is irreducible, this means that σ is 1-dimensional. Define

$$H = \{x \in G : \sigma(x) = 1\}.$$

Obviously, H is a closed normal proper subgroup of G, and all α_i's belong to a single coset of H, contrary to our assumptions. This proves the lemma.

Proof of Theorem 1.3. Recall that, by Weyl's criterion for well-distribution in compact groups [KN, p. 227], $(a_n)_{n=1}^{\infty}$ is well-distributed if and only if

$$\frac{1}{N-M}\sum_{n=M}^{N-1}\sigma(a_n) \xrightarrow[N-M\to\infty]{} 0 \tag{3.2}$$

for every irreducible unitary representation $\sigma \ne 1$ of G.

Let σ be such a representation. Assume first that $M = cr^h$, $N = (c+1)r^h$ for some c and (large) h. It is easy to see that

$$\sum_{n=M}^{N-1}\sigma(a_n) = \Big(\sum_{i=0}^{r-1}\sigma(\alpha_i)\Big)^h\sigma(a_c).$$

By Lemma 3.1 we see that (3.2) is valid for M, N of this form. A routine approximation argument, based on dividing an arbitrary large interval $[M, N-1]$ into a union of several intervals of the form $[cr^h, (c+1)r^h - 1]$ with large h (or h's) and a (relatively) small leftover, finishes the proof.

Proof of Theorem 1.2. In view of Theorem 2.1, the terms of our sequence which are relatively prime to p (and thus relevant to the theorem) are exactly those for which in the base p expansion of n all digits are at most $(p-1)/2$. Let $r = (p+1)/2$. Define a sequence $(a_n)_{n=1}^{\infty}$ in the group $G = (\mathbb{Z}/p\mathbb{Z})^\times$ as follows: If $n = n_0 + n_1 r + \ldots + n_k r^k$ is the base r expansion of n, then a_n is the residue class of $\binom{2m}{m}$, where $m = n_0 + n_1 p + \ldots + n_k p^k$. The foregoing means that the result of the theorem is equivalent to the sequence $(a_n)_{n=1}^{\infty}$ being well-distributed in G.

Now let $\alpha_i \in G$ be the residue class of $\binom{2i}{i}$ modulo p for $i = 0, 1, \ldots, r-1$. Theorem 2.1 shows that the sequence $(a_n)_{n=1}^{\infty}$ is constructed from the elements α_i in exactly the general manner described in Theorem 1.3. Moreover, the first part of the proof of Theorem 1.1 shows that the elements α_i satisfy the two conditions of Theorem 1.3, so that the sequence $(a_n)_{n=1}^{\infty}$ is indeed well-distributed in G. This proves the theorem.

4. Related open problems. Our results deal with the behaviour of the binomial coefficients $\binom{2n}{n}$ modulo prime powers. It is natural to inquire how they behave modulo other integers. The only result in this direction of which we are aware is due to Erdős, Graham, Ruzsa and Straus [EGRS], who proved that the sequence $\binom{2n}{n}$ assumes infinitely often values which are relatively prime to 15, or, more generally, relatively prime to pq, where p and q are distinct odd primes. Thus, considering the modulus 15, for example, it is a simple matter to show (as mentioned in Section 1) that most terms in our sequence are 0 modulo 15. Theorem 1.1 implies that each of the sets $\{1,4,7,10,13\}$, $\{2,5,8,11,14\}$, $\{1,6,11\}$, $\{2,7,12\}$, $\{3,8,13\}$ and $\{4,9,14\}$ contains, modulo 15, infinitely many terms of our sequence. The result of Erdős *et al.* shows the same for the set $\{1,2,4,7,8,11,13,14\}$.

While the result of Erdős *et al.* is similar in spirit to the results of this paper, the underlying ideas used in the proofs are completely different. As is clear from our exposition, the candidates for satisfying the assertion of Theorem 1.1 are numbers whose base p expansion is simple to describe. What is needed is to understand the behaviour of the coefficients $\binom{2n}{n}$ for these candidates n. The problem of [EGRS] is to show that the sets of numbers n corresponding to two distinct primes p and q intersect at an infinite set. Thus it is unlikely that our methods may be applied to questions of the type studied in [EGRS]. For example, it is natural to expect that, say, $\binom{2n}{n}$ belongs infinitely often to each residue class modulo 15. However, the question cannot be tackled using the methods of this paper (nor does it seem to follow in an easy way using the methods of [EGRS]).

In conclusion, it may be of interest to mention here the following question of Graham, which carries a \$1,000 prize [Grah].

QUESTION. Is $\left(\binom{2n}{n}, 105\right) = 1$ for infinitely many positive integers n?

References

[BG] D. Barbolosi et P. J. Grabner, *Distribution des coefficients multinomiaux et q-binomiaux modulo p*, Indag. Math. 7 (1996), 129–135.

[E] P. Erdős, *On some divisibility properties of* $\binom{2n}{n}$, Canad. Math. Bull. 7 (1964), 513–518.

[EG] P. Erdős and R. L. Graham, *Old and New Problems and Results in Combinatorial Number Theory*, L'Enseignement Mathématique, Imprimerie Kundig, Geneva, 1980.

[EGRS] P. Erdős, R. L. Graham, I. Z. Ruzsa and E. G. Straus, *On the prime factors of* $\binom{2n}{n}$, Math. Comp. 29 (1975), 83–92.

[EK] P. Erdős and G. Kolesnik, *Prime power divisors of binomial coefficients*, preprint.

[Ga] A. Gardiner, *Four problems on prime power divisibility*, Amer. Math. Monthly 95 (1988), 926–931.

[GW] R. Garfield and H. S. Wilf, *The distribution of the binomial coefficients modulo p*, J. Number Theory 41 (1992), 1–5.

[Grah] R. Graham, personal communication.

[Gran] A. Granville, *Zaphod Beeblebrox's brain and the fifty-ninth row of Pascal's triangle*, Amer. Math. Monthly 99 (1992), 318–331.

[GR] A. Granville and O. Ramaré, *Explicit bounds on exponential sums and the scarcity of squarefree binomial coefficients*, Mathematika 43 (1996), 73–107.

[Hex] E. Hexel, *Einige Bemerkungen zum Pascal'schen Dreieck modulo p*, in Contributions to Graph Theory and its Applications (International Colloquium Oberhof, 1977), Technische Hochschule Ilmenau, Ilmenau, 1977, 121–128.

[HS] E. Hexel and H. Sachs, *Counting residues modulo a prime in Pascal's triangle*, Indian J. Math. 20 (1978), 91–105.

[Hey] H. Heyer, *Probability Measures on Locally Compact Groups*, Springer, Berlin, 1977.

[KN] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, Wiley, New York, 1974.

[K] E. E. Kummer, *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*, J. Reine Angew. Math. 44 (1852), 93–146.

[L] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. 1 (1878), 184–240, 289–321.

[N] W. Narkiewicz, *Uniform Distribution of Sequences of Integers in Residue Classes*, Lecture Notes in Math. 1087, Springer, Berlin, 1984.

[R] M. Rosenblatt, *Markov Processes. Structure and Asymptotic Behavior*, Springer, Berlin, 1971.

[San] J. W. Sander, *Prime power divisors of* $\binom{2n}{n}$, J. Number Theory 39 (1991), 65–74.

[Sár] A. Sárközy, *On divisors of binomial coefficients*, *I*, ibid. 20 (1985), 70–80.

[V] G. Velammal, *Is the binomial coefficient* $\binom{2n}{n}$ *squarefree?*, Hardy-Ramanujan J. 18 (1995), 23–45.

Department of Mathematics and Computer Science
Ben-Gurion University
Beer-Sheva 84105, Israel
E-mail: berend@black.bgu.ac.il

Tracor Applied Sciences
Building 1-8
6500 Tracor Lane
Austin, Texas 78725
U.S.A.

Received on 29.1.1997
and in revised form on 18.8.1997 (3124)