ACTA ARITHMETICA
127.3 (2007)

On the distribution of $\binom{Cn}{Dn}$ modulo p

by

YOSSI MOSHE (Jerusalem)

1. INTRODUCTION

The behavior of binomial coefficients modulo primes attracted attention for a long time, and still does (cf. [1], [3], [5], [7]–[9]). A classical and very elegant result of Lucas is

THEOREM A ([14]). *Let p be a prime and n, k nonnegative integers, $n \geq k$, with base p representations $[n]_p = n_{l-1} \ldots n_0$, $[k]_p = k_{t-1} \ldots k_0$. Then*

$$\binom{n}{k} \equiv \binom{n_{l-1}}{k_{l-1}} \cdots \binom{n_1}{k_1}\binom{n_0}{k_0} \pmod{p}$$

(*where we agree to put $k_i = 0$ for $i > t-1$ and $\binom{n_i}{k_i} = 0$ if $n_i < k_i$*).

Assume that p is an odd prime and consider the sequence of middle binomial coefficients $A_n = \binom{2n}{n}$. Using Lucas' theorem, one can easily prove that $\binom{2n}{n} \not\equiv 0 \pmod{p}$ if and only if the base p representation of n is composed only of the digits $0, 1, \ldots, (p-1)/2$. Thus, the set of integers n with $\binom{2n}{n} \not\equiv 0 \pmod{p}$ is an infinite set of density 0. Berend and Harmse [4] considered the sequence $(A'_k)_{k=0}^{\infty}$ obtained from $(A_n \bmod p)_{n=0}^{\infty}$ by omitting the zeros. They proved that each nonzero residue modulo p is visited by $(A'_k)_{k=0}^{\infty}$ with the same asymptotic frequency $1/(p-1)$. In fact, they proved a stronger result, showing that the sequence $(A_n)_{n=0}^{\infty}$ is weakly well-distributed modulo p (see Section 2).

Kriger [11] proved the analogous result for the sequences $A_n = \binom{3n}{n}$ and $A_n = \binom{3n}{n,n,n}$ (for $p \geq 11$).

A significant ingredient of the proofs in [4] and [11] was to show that each nonzero residue is indeed visited by $(A_n)_{n=0}^{\infty}$. The main tool for proving this was the investigation of the function $g(n) = A_{n+1}/A_n$. In fact, it was found

2000 *Mathematics Subject Classification*: Primary 11B50, 11B65, 05A10; Secondary 11K99.

Key words and phrases: binomial coefficients, Pascal's triangle, asymptotic frequency.
Supported in part by FWF Project P16004–N05.

that it is enough to prove that the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^{\times}$ is generated by $\{g(n) : 0 \le n < p/C - 1\}$, where $C = 2$ for the sequence $A_n = \binom{2n}{n}$ and $C = 3$ for $\binom{3n}{n}$ and $\binom{3n}{n,n,n}$.

In this paper, we consider the sequence $A_n = \binom{Cn}{Dn}$ for any constants C, D with $C > D > 0$. It turns out to be difficult to continue with the function $g(n) = A_{n+1}/A_n$ for large values of C. One of the reasons is that (assuming that C, D are coprime) $g(n)$ is a rational function whose numerator and denominator are polynomials of degree $C-1$ in n (for example, if $A_n = \binom{3n}{n}$, then $g(n) = \frac{3(3n+1)(3n+2)}{2(n+1)(2n+1)}$). Thus, $g(n)$ becomes more and more complicated as C grows. In addition, the interval $[0, p/C - 1)$ becomes smaller.

The key observation in our proof is that the behavior of $\binom{Cn}{Dn} \pmod p$ is related to the Möbius transformation $f(n) = (Cn + 1)/(Dn + 1)$. We find that $f(n)$ can play (under certain assumptions on C, D) a role similar to the function $g(n)$ in [4], [11]. This observation enables us to generalize the above mentioned results to each of the sequences $A_n = \binom{Cn}{Dn}$.

We also study the behavior of more general sequences modulo p. For example, we consider multinomial sequences of the form $A_n = \binom{Kn}{K_1 n, \ldots, K_t n}$, as well as sequences in $\mathbb{Z}^d$, defined in terms of binomial coefficients.

In Section 2 we formulate our main results. In Section 3 we consider the set of nonzero residues modulo p which are visited by $\binom{Cn}{Dn} \pmod p$ and in Section 4 we prove that each such residue is visited with the same asymptotic frequency (when ignoring the 0's).

2. THE MAIN RESULTS

Let p be a prime. A sequence $\vec{A} = (A_n)_{n=0}^{\infty}$ over $\mathbb{Z}$ is *p-solvable* if for every $r \in \mathbb{Z}/p\mathbb{Z}$ there exist infinitely many solutions n for the congruence $A_n \equiv r \pmod p$.

Consider the sequence $A_n = \binom{Cn}{Dn}$, where C, D are arbitrary integers with $0 < D < C$. Let ν_p denote the p-adic valuation (that is, $p^{\nu_p(n)}$ is the exact power of p dividing n). It can be easily observed (see Lemma 10) that, if $\nu_p(C) > \nu_p(D)$, then $\binom{Cn}{Dn} \equiv 0 \pmod p$ for every $n > 0$. In particular, $\binom{Cn}{Dn}$ is not p-solvable. Our key result is

Theorem 1. *Let $p > 5$ be a prime and C, D integers with $0 < D < C$. Then $\binom{Cn}{Dn}$ is p-solvable if and only if $\nu_p(C) \le \nu_p(D)$.*

In particular, considering also a few cases with $p = 3, 5$, we obtain

Corollary 2. *Let C, D be integers with $0 < D < C$. Then $\binom{Cn}{Dn}$ is p-solvable for every prime $p > C$, with the exception of the case $(C, D, p) = (4, 2, 5)$.*

COROLLARY 3. *For any $C \geq 2$, the sequence $\binom{Cn}{n}$ is p-solvable if and only if p does not divide C.*

We note that Theorem 1 is false in general for $p = 3, 5$. In fact, for these primes, taking $C = 4$ and $D = 2$, we see that the quadratic residues modulo p (including 0) are the only possible values for $\binom{Cn}{Dn} \pmod p$. In particular, $\binom{Cn}{Dn}$ is not p-solvable. Note that this implies that $A_n = \binom{2Dn}{Dn}$ is not p-solvable for any even integer D and $p = 3, 5$.

OPEN QUESTION 4. Let $p = 3, 5$. For which values of C, D is the sequence $\binom{Cn}{Dn}$ p-solvable?

Let us now consider the relative frequency with which each nonzero residue is visited by $(A_n \bmod p)_{n=0}^{\infty}$. In this part we consider more general sequences than in Theorem 1. We begin with a few notations.

Take a sequence $\vec{A} = (A_n)_{n=0}^{\infty}$ in $\mathbb{Z}$ and denote by $S = S(\vec{A})$ the set of nonzero residues $r \in (\mathbb{Z}/p\mathbb{Z})^{\times}$ such that $A_n \equiv r \pmod p$ for infinitely many n's. Assume that $S \neq \emptyset$ and let $(A'_k)_{k=0}^{\infty}$ denote the subsequence of $(A_n \bmod p)_{n=0}^{\infty}$ obtained by omitting the zeros. The sequence $(A_n)_{n=0}^{\infty}$ is *S-weakly uniformly distributed modulo p* (cf. [16, p. 8]) if each $r \in S$ appears in $(A'_n)_{n=0}^{\infty}$ with the same asymptotic frequency $1/\#(S)$. More precisely, let the *density* of a set $X \subseteq \mathbb{N}$ be

$$D(X) = \lim_{N\to\infty} \frac{\#([0, N) \cap X)}{N}$$

(if the limit exists). Then $(A_n)_{n=0}^{\infty}$ is S-weakly uniformly distributed modulo p if $D(\{n \in \mathbb{N} : A'_n = r\}) = 1/\#(S)$ for every $r \in S$.

We also define a stronger version of uniform distribution modulo p, where we demand the limit to be valid for any "large" intervals $[N, M)$ and not only for initial intervals $[0, N)$. Let the *Banach density* (cf. [6, p. 72]) of a set $X \subseteq \mathbb{N}$ be

$$BD(X) = \lim_{M-N\to\infty} \frac{\#([N, M) \cap X)}{M - N}$$

(if the limit exists). Then $(A_n)_{n=0}^{\infty}$ is *S-weakly well-distributed modulo p* (cf. [12, p. 84, p. 200, p. 221]) if $BD(\{n \in \mathbb{N} : A'_n = r\}) = 1/\#(S)$ for every $r \in S$.

Take a multinomial sequence of the form

$$A_n = \binom{Kn}{K_1 n, \ldots, K_m n}, \tag{1}$$

where K_i are positive integers with $\sum_{i=1}^{m} K_i = K$. Assume that $A_n \not\equiv 0 \pmod p$ for some positive n and define

$$G = \{A_n \bmod p : n \geq 1\} \setminus \{0\} \subseteq (\mathbb{Z}/p\mathbb{Z})^{\times}.$$

LEMMA 5. *Let* $(A_n)_{n=0}^{\infty}$ *be as in* (1). *Then*:

(i) *G is a subgroup of* $(\mathbb{Z}/p\mathbb{Z})^{\times}$.
(ii) *Each residue* $r \in G$ *is visited by* $(A_n \bmod p)_{n=0}^{\infty}$ *infinitely often.*
(iii) *The set* $\{n \in \mathbb{N} : A_n \not\equiv 0 \pmod p\}$ *is of Banach density* 0.

THEOREM 6. *The sequence* (A_n) *in* (1) *is G-weakly well-distributed modulo p.*

EXAMPLE 7. If $A_n = \binom{3n}{n,n,n}$ and $p = 7$, then $G = \{1, 6\}$, and thus the residues $1, 6$ are visited by (A'_n) with the same asymptotic frequency $1/2$.

We also provide analogues of Lemma 5 and Theorem 6 for multiple binomial sequences in $\mathbb{Z}^m$.

THEOREM 8. *Let* $C_1, D_1, \ldots, C_m, D_m$ *be integers with* $C_i > D_i > 0$ *and*

$$A_n = \left(\binom{C_1 n}{D_1 n}, \ldots, \binom{C_m n}{D_m n}\right) \in \mathbb{Z}^m, \qquad n \geq 0.$$

Assume that $G = \{A_n \bmod p : n \geq 1\} \cap ((\mathbb{Z}/p\mathbb{Z})^{\times})^m$ *is nonempty* (*where* $A_n \bmod p$ *denotes the m-vector obtained from A_n by taking the residue modulo p of each coordinate*). *Then*:

(i) *G is a subgroup of* $((\mathbb{Z}/p\mathbb{Z})^{\times})^m$.
(ii) *For each* $r \in G$ *there are infinitely many n's with* $A_n \equiv r \pmod p$.
(iii) $BD(\{n \in \mathbb{N} : A_n \in ((\mathbb{Z}/p\mathbb{Z})^{\times})^m \pmod p\}) = 0$.
(iv) *Let* $(A'_n)_{n=0}^{\infty}$ *be the sequence obtained from* $(A_n \bmod p)_{n=0}^{\infty}$ *by omitting those elements* $A_n \bmod p$ *not belonging to* $((\mathbb{Z}/p\mathbb{Z})^{\times})^m$. *Then*

$$BD(\{n \in \mathbb{N} : A'_n = r\}) = 1/\#(G), \qquad r \in G.$$

3. THE SET $\{\binom{Cn}{Dn} \bmod p : n \geq 1\} \setminus \{0\}$

In this section C, D are fixed integers with $0 < D < C$, and p is a prime. We start with a few notations and basic lemmas.

Let Ω be a finite set. A *word* w of *length* $l = l(w) \geq 0$ over Ω is a concatenation of l elements in Ω (called *letters*). Write Λ for the empty word. Let wz denote the concatenation of two words w, z over Ω and w^k the concatenation of w with itself $k \geq 0$ times. Thus for example, $1(10)^2 01^3 = 110100111$ is a word of length 9 over $\Omega = \mathbb{Z}/2\mathbb{Z}$. A word z is a *subword* of w if $w = z_0 z z_1$ for some words z_0, z_1.

The *base p representation* of an integer $n > 0$ is the (unique) word $[n]_p = n_{l-1} \ldots n_1 n_0$ over $\mathbb{Z}/p\mathbb{Z}$ with $n = \sum_{i=0}^{l-1} n_i p^i$ and $n_{l-1} \neq 0$. We will refer to n_0, n_{l-1} as the *least significant*, and *most significant digits* of n, respectively, and to n_i as the *ith digit* (where we agree that $n_i = 0$ for $i \geq l$). Put $[0]_p = \Lambda$.

Let $k \le n$ be a nonnegative integer with base p representation $k_{t-1}\dots k_1k_0$. We write $k \preceq n$ if $k_i \le n_i$ for each i. (By Lucas' theorem we have $p \nmid \binom{n}{k}$ if and only if $k \preceq n$.) Write $l(n) = l([n]_p)$.

LEMMA 9. *Let $n, n_0, n_1 > 0$ be integers and assume $[n]_p = [n_0]_p 0^l [n_1]_p$ for some $l \ge l(C)$. Then*

$$\binom{Cn}{Dn} \equiv \binom{Cn_0}{Dn_0}\binom{Cn_1}{Dn_1} \pmod{p}.$$

The lemma follows directly from Lucas' theorem upon observing that

$$[Cn]_p = [Cn_0]_p 0^i [Cn_1]_p, \qquad [Dn]_p = [Dn_0]_p 0^j [Dn_1]_p$$

for some $i, j \ge 0$ satisfying $i + l(Cn_1) = j + l(Dn_1) = l + l(n_1)$.

Put

$$G = \left\{ \binom{Cn}{Dn} \bmod p : n \ge 1 \right\} \setminus \{0\}.$$

LEMMA 10.

(i) *G is either empty or a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$.*
(ii) *$G = \emptyset$ if and only if $\nu_p(C) > \nu_p(D)$.*

Proof. (i) Since, by Lemma 9, G is closed under multiplication, it is either empty or a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$.

(ii) Assume first that $\nu_p(C) > \nu_p(D)$. Let $n \ge 1$ and $i = \nu_p(Dn)$. The ith digit of Cn is 0, whereas the ith digit of Dn is not. By Lucas' theorem, $\binom{Cn}{Dn} \equiv 0 \pmod{p}$, and so $G = \emptyset$.

Assume now that $\nu_p(C) \le \nu_p(D)$. By Lucas' theorem, $\binom{C'n}{D'n} \equiv \binom{C'p^i n}{D'p^i n} \pmod{p}$ for every C', D', i. Dividing C and D by an appropriate power of p, we may assume that $C \not\equiv 0 \pmod{p}$. Put $m = (p^{\phi(C)} - 1)/C$, where ϕ is Euler's totient function, and note that m is an integer. Since the word $[Cm]_p$ consists of occurrences of the letter $p-1$ only, we have $Dm \preceq Cm$, and thus $\binom{Cm}{Dm} \not\equiv 0 \pmod{p}$. In particular, $G \ne \emptyset$. ∎

LEMMA 11. *For every $r \in G \cup \{0\}$, there are infinitely many n's such that $\binom{Cn}{Dn} \equiv r \pmod{p}$. In particular, if $G = (\mathbb{Z}/p\mathbb{Z})^\times$, then $\binom{Cn}{Dn}$ is p-solvable.*

Proof. We first prove the existence of an $n' > 0$ with $\binom{Cn'}{Dn'} \equiv 0 \pmod{p}$. Take an integer $a > 0$ such that $C/p^a \le \min(D, C-D)$ and put $n' = \lceil p^l/C \rceil$ for some $l \ge a + l(C)$. Note that $Cn' \in [p^l, p^l + C)$, and thus $[Cn']_p = 10^a w$ for some word w. Since $C/p^a \le D$ and so $p^a Dn' \ge Cn'$, we get

$$l(Dn') \ge l(Cn') - a = l(w) + 1.$$

Similarly, since $C/p^a \le C - D$ and so $p^a Dn' \le (p^a - 1)Cn'$ we get

$$l(Dn') \le l((p^a - 1)Cn') - a = l(Cn') - 1.$$

Taking $l = l(Dn') - 1 \in [l(w), l(Cn') - 2]$, we infer that the lth digit of Cn' is 0, whereas the lth digit of Dn' is not. By Lucas' theorem we have $\binom{Cn'}{Dn'} \equiv 0 \pmod{p}$.

Now let $r \in G \cup \{0\}$ and n be such that $\binom{Cn}{Dn} \equiv r \pmod{p}$. Lucas' theorem shows that $\binom{Cnp^i}{Dnp^i} \equiv r \pmod{p}$ for every i. ∎

Lemma 12. *Let $n_0, n_1 > 0$ be integers. Denote by c_0, d_0 the least significant digits of Cn_0, Dn_0, respectively, and by c_1, d_1 the lth digits of Cn_1, Dn_1, respectively, where $l = l(Cn_1) - 1$. Assume that $Dn_i \preceq Cn_i$ for $i = 0, 1$ and that $c_0 + c_1 < p$. Then*

$$\frac{\binom{c_0+c_1}{d_0+d_1}}{\binom{c_0}{d_0}\binom{c_1}{d_1}} \in G.$$

Proof. Take words w_0, w_1, z_0, z_1 over $\mathbb{Z}/p\mathbb{Z}$ such that

$$[Cn_0]_p = w_0c_0, \quad [Dn_0]_p = z_0d_0, \quad [Cn_1]_p = c_1w_1, \quad 0^a[Dn_1]_p = d_1z_1,$$

where $a = l(Cn_1) - l(Dn_1)$. Put $n = n_0p^l + n_1$, and note that

$$[Cn]_p = w_0(c_0 + c_1)w_1, \qquad [Dn]_p = z_0(d_0 + d_1)z_1.$$

Using Lucas' theorem we obtain

$$\frac{\binom{Cn}{Dn}}{\binom{Cn_0}{Dn_0}\binom{Cn_1}{Dn_1}} = \frac{\binom{c_0+c_1}{d_0+d_1}}{\binom{c_0}{d_0}\binom{c_1}{d_1}} \in G. \ ∎$$

3.1. Proof of Theorem 1, assuming $D \not\equiv 0, C/2, C \pmod{p}$. In this subsection we prove Theorem 1 for the cases where

(i) $D \not\equiv 0, C/2, C \pmod{p}$.

In this part of the proof, p may also be 5. The cases $D \equiv 0, C/2, C \pmod{p}$ will be handled in Subsection 3.2 for $p > 5$. It will also be convenient to add the following two assumptions on C, D:

(ii) $C = p^e - 1$ for some positive integer e,
(iii) $C/2 < D < C$.

To justify assumptions (ii), (iii), observe the following. Lemma 10 shows that the assertion of Theorem 1 is true in the cases where $\nu_p(C) > \nu_p(D)$. Thus we may assume $\nu_p(C) \le \nu_p(D)$. Since, by assumption (i), $\nu_p(D) = 0$, we conclude that C is not a multiple of p. Replacing the pair (C, D) with (Cm, Dm), where m is as in the proof of Lemma 10, we obtain (ii). In order to obtain (iii), we replace (if necessary) the pair (C, D) with $(C, C - D)$. Note that, if we replace (C, D) with (C', D') according to the above two cases, then (C', D') still satisfies assumption (i). Moreover, if $\binom{C'n}{D'n}$ is p-solvable, then so is $\binom{Cn}{Dn}$. Thus, without loss of generality, we may assume (i)–(iii).

In our proof we will repeatedly use properties of Möbius transformations. A *Möbius transformation* over a field $\mathbb{F}$ is a rational function of the form $f(n) = (an+b)/(cn+d)$, where the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is invertible. A very basic property of a Möbius transformation f is that it permutes the elements of $\mathbb{F} \cup \{\infty\}$ (when we put $f(\infty) = a/c$, $f(-d/c) = \infty$). We refer the reader to [17] for more on Möbius transformations.

Let f be the Möbius transformation over $\mathbb{Z}/p\mathbb{Z}$ given by

$$f(n) = \frac{Cn+1}{Dn+1}.$$

By assumption (ii) we have $f(n) = (-n+1)/(Dn+1)$. Define

$$T = \left\{0 \le n < p : n \ne 1, \binom{Cn}{Dn} \not\equiv 0 \pmod{p}\right\}.$$

Observe that assumption (ii) implies

LEMMA 13. *Let $k \le C$ be a positive integer, and put $l_0 = l(k)$ and $l_1 = l(p^{l_0} - k)$. Then*

$$[kC]_p = [k-1]_p (p-1)^{e-l_0} 0^{l_0 - l_1} [p^{l_0} - k]_p.$$

PROPOSITION 14. *$G \supseteq f(T)$.*

Proof. Let $n \in T$. Since G is a group, we obtain $f(0) = 1 \in G$. Thus we may assume $n \ne 0$. By Lemma 13 we have $[2C]_p = 1(p-1)^{e-1}(p-2)$. Since $C/2 < D < C$, the word $[2D]_p$ is of the same length as $[2C]_p$, and it begins with 1 as well. Write

$$[Cn]_p = w_0 c, \quad [Dn]_p = z_0 d, \quad [2C]_p = 1w_1, \quad [2D]_p = 1z_1,$$

where c, d are the residues of Cn, Dn modulo p, respectively.

The assumption $D \not\equiv C/2 \pmod{p}$ ensures that the least significant digit of $2D$ is not $p-1$. Thus, $2D \preceq 2C$. Since $n \in T$, we have $Dn \preceq Cn$. Note that $C \equiv -1 \pmod{p}$ and $n \ne 1$. Thus, $c \ne p-1$ as $1 < n < p$ and so $c+1 < p$. Lemma 12 yields

$$\frac{c+1}{d+1} = \frac{\binom{c+1}{d+1}}{\binom{c}{d}\binom{1}{1}} \in G.$$

Since $c \equiv Cn \pmod{p}$ and $d \equiv Dn \pmod{p}$, we get $(Cn+1)/(Dn+1) \in G$. ∎

LEMMA 15. *For every integer $n \in [1, p-1]$, we have $\binom{Cn}{Dn} \not\equiv 0 \pmod{p}$ if and only if $\binom{C(p-n)}{D(p-n)} \equiv 0 \pmod{p}$.*

Proof. Let d denote the least significant digit of Dn. Recall that, by Lucas' theorem, we have $\binom{Cn}{Dn} \not\equiv 0 \pmod{p}$ if and only if $Dn \preceq Cn$. Since $[Cn]_p = (n-1)(p-1)^{e-1}(p-n)$, this happens if and only if $d \le p-n$.

Similarly, observing that the least significant digits of $C(p-n)$, $D(p-n)$ are $n, p-d$, respectively, we obtain $\binom{C(p-n)}{D(p-n)} \equiv 0 \pmod{p}$ if and only if $p-d>n$.

By the assumption $D \not\equiv C \pmod{p}$ we have $Dn \not\equiv Cn \pmod{p}$, and so $d \neq p-n$. Thus the conditions $d \leq p-n$ and $p-d>n$ are equivalent. ∎

Lemma 16. *T is of cardinality $(p-1)/2$.*

Proof. By the previous lemma, $\binom{Cn}{Dn} \not\equiv 0 \pmod{p}$ for exactly $(p-1)/2$ of the elements $n \in [1, p-1]$. One of those values is $n=1$, which does not belong to T. On the other hand, $0 \in T$, which gives $\#(T) = (p-1)/2$. ∎

Denote the set of nonzero quadratic residues modulo p by Q, and let $\overline{Q} = (\mathbb{Z}/p\mathbb{Z})^{\times} \setminus Q$ denote the set of quadratic nonresidues.

Corollary 17. *G contains at least $(p-1)/2$ elements. In particular, either $G = Q$ or $G = (\mathbb{Z}/p\mathbb{Z})^{\times}$.*

In fact, this follows from the injectivity of f, Proposition 14 and Lemma 16.

Lemma 18. *If $G \neq (\mathbb{Z}/p\mathbb{Z})^{\times}$, then $G = f(T)$.*

Proof. By Proposition 14, $f(T) \subseteq G$. Note that if $f(T) \subsetneq G$, then $\#(G) > (p-1)/2$, and so $G = (\mathbb{Z}/p\mathbb{Z})^{\times}$. Thus, we must have $f(T) = G$. ∎

Let $h(n)$ be the rational function on $\mathbb{Z}/p\mathbb{Z}$ given by

$$h(n) = f(n)f(-n) = \frac{n^2-1}{D^2n^2-1}.$$

Proposition 19. *Assume that $G \neq (\mathbb{Z}/p\mathbb{Z})^{\times}$ and let $n \in (\mathbb{Z}/p\mathbb{Z})^{\times}$ be such that $n^2-1 \neq 0$ and $D^2n^2-1 \neq 0$. Then $h(n) \in \overline{Q}$.*

Proof. By Corollary 17 we have $G = Q$. By our assumptions $n \neq \pm 1$. Thus, Lemma 15 shows that exactly one of the elements $n, p-n$ belongs to T. By Lemma 18 and the fact that f is an injection we see that exactly one of $f(n), f(p-n)$ belongs to G, and we conclude that one of them is a quadratic residue modulo p and the other is not. In particular, $f(n)f(-n) \in \overline{Q}$. ∎

Remark. Let $\phi(n) = \left(\frac{n}{p}\right)$ denote the Legendre symbol of n modulo p and put $M(x) = (x^2-1)(D^2x^2-1) \in \mathbb{Z}/p\mathbb{Z}[x]$. An equivalent formulation of Proposition 19 is that, assuming $G \neq (\mathbb{Z}/p\mathbb{Z})^{\times}$, we have $\phi(M(n)) = -1$ for every $n \in (\mathbb{Z}/p\mathbb{Z})^{\times}$ which is not a root of $M(x)$. Observing that $\phi(M(0)) = 1$, we get

$$\sum_{n \in \mathbb{Z}/p\mathbb{Z}} \phi(M(n)) \leq -(p-6). \tag{2}$$

One way to use Proposition 19 for proving Theorem 1 for $p > 19$ and $D \not\equiv 0, C/2, C \pmod{p}$ is to observe that (2) contradicts the estimate of

$\sum_{n\in\mathbb{Z}/p\mathbb{Z}}\phi(M(n))$ given in [13, Thm. 5.41] for those values of p. A self-contained proof of Theorem 1 for those cases is given below.

LEMMA 20. *If* (C,D,p) *satisfies assumptions* (i)–(iii) *and* p *is a prime number in* $[5,19]$, *then* $\binom{Cn}{Dn}$ *is* p*-solvable.*

Proof. By Proposition 14 it suffices to prove that $f(T)$ generates $(\mathbb{Z}/p\mathbb{Z})^\times$. Assume first that $(D,p)\notin(2+7\mathbb{Z},7)$ and $(D,p)\notin(2+13\mathbb{Z},13)$. Table 1 provides a number $n\in T$ such that $f(n)$ generates $(\mathbb{Z}/p\mathbb{Z})^\times$. For the case $p=13$, $D\equiv 2 \pmod{13}$, observe that $2,3\in T$ and that $\{f(2),f(3)\}=\{5,9\}$ generates $\mathbb{Z}/13\mathbb{Z}$.

Assume $p=7$ and $D\equiv 2 \pmod 7$. Note that

$$[4C]_p = 36^{e-1}3, \qquad [4D]_p = aw1,$$

where $a\in\{2,3\}$ and w is a word of length $e-1$. Using Lemma 12 (with $n_0=n_1=4$) we infer that $g=\binom{6}{a+1}/\binom{3}{a}\binom{3}{1}$ belongs to G. Since $a\in\{2,3\}$, we have $g\in\{3,5\} \pmod p$, and so g generates $(\mathbb{Z}/p\mathbb{Z})^\times$. ∎

Table 1. A number $n\in T$ such that $f(n)$ generates $(\mathbb{Z}/p\mathbb{Z})^\times$ for $5\le p\le 19$

$D\diagdown p$	$p=5$	$p=7$	$p=11$	$p=13$	$p=17$	$p=19$
$D\equiv 1 \pmod p$	$f(2)=3$	$f(3)=3$	$f(2)=7$	$f(3)=6$	$f(2)=11$	$f(6)=2$
$D\equiv 2 \pmod p$	$D\equiv C/2$		$f(2)=2$		$f(2)=10$	$f(2)=15$
$D\equiv 3 \pmod p$	$f(2)=2$	$D\equiv C/2$	$f(5)=8$	$f(2)=11$	$f(2)=12$	$f(3)=15$
$D\equiv 4 \pmod p$	$D\equiv C$	$f(2)=3$	$f(2)=6$	$f(5)=6$	$f(6)=10$	$f(2)=2$
$D\equiv 5 \pmod p$		$f(2)=5$	$D\equiv C/2$	$f(2)=7$	$f(2)=3$	$f(5)=13$
$D\equiv 6 \pmod p$		$D\equiv C$	$f(3)=8$	$D\equiv C/2$	$f(4)=6$	$f(7)=14$
$D\equiv 7 \pmod p$			$f(2)=8$	$f(2)=6$	$f(3)=3$	$f(4)=13$
$D\equiv 8 \pmod p$			$f(7)=8$	$f(4)=7$	$D\equiv C/2$	$f(2)=10$
$D\equiv 9 \pmod p$			$f(3)=7$	$f(2)=2$	$f(3)=6$	$D\equiv C/2$
$D\equiv 10 \pmod p$			$D\equiv C$	$f(8)=2$	$f(3)=12$	$f(3)=3$
$D\equiv 11 \pmod p$				$f(4)=6$	$f(2)=14$	$f(2)=14$
$D\equiv 12 \pmod p$				$D\equiv C$	$f(3)=5$	$f(2)=3$
$D\equiv 13 \pmod p$					$f(2)=5$	$f(4)=15$
$D\equiv 14 \pmod p$					$f(2)=7$	$f(6)=10$
$D\equiv 15 \pmod p$					$f(2)=6$	$f(3)=14$
$D\equiv 16 \pmod p$					$D\equiv C$	$f(4)=2$
$D\equiv 17 \pmod p$						$f(2)=13$
$D\equiv 18 \pmod p$						$D\equiv C$

Let $X\subseteq Q$, $Y\subseteq\overline{Q}$. A function $g:\mathbb{Z}/p\mathbb{Z}\cup\{\infty\}\to\mathbb{Z}/p\mathbb{Z}\cup\{\infty\}$ *exchanges* Q, $\overline{Q}$ *with possible exceptions* (X,Y) if $g(x)\in\overline{Q}$ for every $x\in Q\setminus X$ and $g(x)\in Q$ for every $x\in\overline{Q}\setminus Y$.

Proof of Theorem 1 for $D \not\equiv 0, C/2, C \pmod p$. Suppose the sequence $\binom{Cn}{Dn}$ is not p-solvable for some C, D with $\nu_p(C) \le \nu_p(D)$. By Lemma 11, Corollary 17 and Lemma 20, we have $p > 19$ and $G = Q$. If $D^2 \equiv 1 \pmod p$, then the function h is identically 1, which contradicts Proposition 19. Therefore $D^2 \not\equiv 1 \pmod p$. Consider the Möbius transformation

$$g(x) = \frac{x-1}{D^2x-1}.$$

Proposition 19 shows that $g(x) \in \overline{Q}$ for every $x \in Q \setminus \{1, 1/D^2\}$. Observe that $g(0), g(\infty) \in Q$. Since g is a Möbius transformation, it is a permutation of $\mathbb{Z}/p\mathbb{Z} \cup \{\infty\}$. This implies that there exist $a, b \in \overline{Q}$ such that g exchanges Q, $\overline{Q}$ with exceptions $(\{1, 1/D^2\}, \{a, b\})$.

Multiplying $g(x)$ by $((D^2x-1)/D)^2$, we conclude that the polynomial

$$P(x) = g(x)\left(\frac{D^2x-1}{D}\right)^2 = (x-1)\left(x - \frac{1}{D^2}\right)$$

exchanges Q, $\overline{Q}$ with the same exceptions. Set

$$d = \frac{1}{2}(1 + 1/D^2) \in \mathbb{Z}/p\mathbb{Z}.$$

Assume first $d \neq 0$. Observe that $P(x+d) = P(-x+d)$ for every $x \in \mathbb{Z}/p\mathbb{Z}$. Since P exchanges Q, $\overline{Q}$, we conclude that, for each $x \in \mathbb{Z}/p\mathbb{Z}$ which is not one of the following (up to) ten possible exceptions:

$$E = \{\pm(r-d) : r \in \{1, 1/D^2, a, b, 0\}\},$$

we have $x + d \in Q$ if and only if $-x + d \in Q$, and similarly for $\overline{Q}$. Consider the Möbius transformation $M(x) = (x+d)/(-x+d)$. We obtain $M(x) \in Q$ for every $x \in \mathbb{Z}/p\mathbb{Z} \setminus E$. Since M is injective and $p > 19$, this gives a contradiction.

Now assume $d = 0$. In this case $D^2 \equiv -1 \pmod p$, and thus $P(x) = x^2 - 1$ exchanges Q, $\overline{Q}$ with the exceptions $(\{1, -1\}, \{a, b\})$.

Since $p > 19$, we get $9 \in Q \setminus \{\pm 1\}$, and so $80 = 9^2 - 1 \in \overline{Q}$. Since $80 = 4^2 \cdot 5$, we conclude that $5 \in \overline{Q}$. Now $4 \in Q \setminus \{\pm 1\}$, and thus $15 = 4^2 - 1 \in \overline{Q}$. Since $5 \in \overline{Q}$, we obtain $3 \in Q$. Hence $8 = 3^2 - 1 \in \overline{Q}$, which implies that $2 \in \overline{Q}$. Since $2, 5 \in \overline{Q}$, we have $10 \in Q$, which gives $99 = 10^2 - 1 \in \overline{Q}$, and so $11 \in \overline{Q}$. Since $3 \in Q$, we have $12 \in Q$, and thus $11 \cdot 13 = 12^2 - 1 \in \overline{Q}$, and since $11 \in \overline{Q}$ we conclude $13 \in Q$. Finally, $25 \in Q$, and so $2^4 \cdot 3 \cdot 13 = 25^2 - 1 \in \overline{Q}$, which is a contradiction. ∎

3.2. Proof of Theorem 1 for $D \equiv 0, C/2, C \pmod p$. We begin with the case $D \equiv C/2 \pmod p$. Exactly as before, we may assume $C = p^e - 1$ for some e.

PROPOSITION 21. *If $D \equiv C/2 \pmod p$, then $\binom{Cn}{Dn}$ is p-solvable for $p \ge 7$.*

Proof. Replacing (C,D) with $(C,C-D)$, we may assume $D \le C/2$. Define $I = [0,(p-3)/2]$ (where $[a,b]$ denotes the set of integers k with $a \le k \le b$). Choose $k \in I$ and $t = p-2k$. Note that the least significant digits of Ct, Dt are $2k, k$, respectively, and that the most significant digit of $3C$ is 2. Write

$$[Ct]_p = w_0(2k), \quad [Dt]_p = z_0 k, \quad [3C]_p = 2w_1, \quad 0^a[3D]_p = dz_1,$$

where $a = l(3C) - l(3D)$ and by the assumption $D \le C/2$ we have $d \in \{0,1\}$. Note also that each letter in w_0, except for the leading one, is $p-1$. Thus, $Dt \preceq Ct$, and in particular (taking $k = (p-3)/2$ and so $t = 3$) we have $3D \preceq 3C$.

Assume first that $d = 0$. Lemma 12 yields

$$\frac{2(2k+1)}{k+2} = \frac{\binom{2k+2}{k}}{\binom{2k}{k}\binom{2}{0}} \in G, \qquad k \in I.$$

Taking $k = 1$ we obtain $2 \in G$, and hence $(2k+1)/(k+2) \in G$ for each $k \in I$. If $p = 7$, then, taking $k = 2$, we have $5/4 \in G$, so that $5 \in G$. Since 5 generates $(\mathbb{Z}/7\mathbb{Z})^\times$, this implies the assertion. Assume therefore $p > 7$. Taking $k = 4$, we obtain $3 \in G$. Assume to the contrary that $G \ne (\mathbb{Z}/p\mathbb{Z})^\times$, and let m be the minimal residue in $(\mathbb{Z}/p\mathbb{Z})^\times \setminus G$. Assume first that m is even (when considered as an integer in $[1,p-1]$). Put $k = m/2 \in [1,(p-1)/2]$. Since $2 \in G$ and $m \notin G$, we obtain $k \notin G$, which contradicts the minimality of m. Assume now that m is odd and write $m = 2k+1$. Note that k must belong to I. Since $(2k+1)/(k+2) \in G$, we conclude that $k+2 \notin G$. Since $m \ne 3$, and so $k > 1$, we obtain $k+2 < m$, which contradicts the assumption that m is minimal.

Consider now the case where $d = 1$. Here we obtain

$$\frac{2k+1}{k+1} = \frac{\binom{2k+2}{k+1}}{\binom{2k}{k}\binom{2}{1}} \in G, \qquad k \in I.$$

If $p = 7$, then $3/2 \in G$ is a generator of $(\mathbb{Z}/7\mathbb{Z})^\times$. Assume $p > 7$. We obtain $3/2, 5/3, 9/5 \in G$ and so $2 = (2/3)\cdot(5/3)\cdot(9/5) \in G$. Assume $G \ne (\mathbb{Z}/p\mathbb{Z})^\times$, and let m be the minimal residue in $(\mathbb{Z}/p\mathbb{Z})^\times \setminus G$. As before, m cannot be even. Write $m = 2k+1$. Since $(2k+1)/(k+1) \in G$, we obtain $k+1 \notin G$, which contradicts the minimality of m. ∎

Consider now the cases where $D \equiv 0, C \pmod{p}$. As before, we assume that $C = p^e - 1$. Replacing (if necessary) the pair (C,D) with $(C,C-D)$ we may assume $D \equiv 0 \pmod{p}$. It will be convenient to define $v = \nu_p(D)$ and $R = \lfloor C/D \rfloor + 1$. Note that $v \ge 1$ and that R is the minimal integer with $RD > C$ (and thus minimal with $l(RD) = e+1$).

The proof is broken into the following three lemmas.

Lemma 22. *Assume that $R \le \lceil 2p/3 \rceil + 1$. Then $\binom{Cn}{Dn}$ is p-solvable for every prime $p \ge 7$.*

Proof. Since $p \ge 7$ we have $R < p$. Take an $n_0 < p$ and note that

$$[Cn_0]_p = w_0(p-n_0), \quad [Dn_0]_p = z_0 0, \quad [CR]_p = (R-1)w_1, \quad [DR]_p = 1z_1,$$

for some words w_0, w_1, z_0, z_1 with $l(w_1) = l(z_1) = e$. Since each letter of w_0, except for the leading one, is $p-1$, we get $Dn_0 \preceq Cn_0$ for each $n_0 < p$, and so $DR \preceq CR$ as well. Taking $n_0 \in [R, p-1]$ we obtain $p - n_0 + R - 1 < p$. Thus, Lemma 12 implies

$$\frac{p-n_0+R-1}{R-1} = \frac{\binom{p-n_0+R-1}{1}}{\binom{p-n_0}{0}\binom{R-1}{1}} \in G, \qquad n_0 \in [R, p-1].$$

This shows that

$$\frac{p-n_0+R-1}{p-n_0'+R-1} \in G \qquad \text{for every } n_0, n_0' \in [R, p-1],$$

and so $a/b \in G$ for every $a, b \in [R, p-1]$. In particular, $-a \equiv a/(p-1) \in G$ for every such a. Define $I = [1, p-1-\lceil 2p/3 \rceil]$. Since $R \le \lceil 2p/3 \rceil + 1$, we have $I \subseteq G$.

Assume first that $p \ge 71$. Since $3 \in I$, we obtain $\{3i : i \in I\} \subseteq G$. A simple calculation shows that $\#(I \cup \{3i : i \in I\}) > (p-1)/2$ for $p \ge 71$. Thus, $\#(G) > (p-1)/2$, and hence $G = (\mathbb{Z}/p\mathbb{Z})^\times$. In the cases $11 \le p \le 67$ it can be checked that there exists a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$ in the interval I.

We are left with the case $p = 7$. If $R \le 5$, then it can be easily verified that

$$\left\{ \frac{p-n_0+R-1}{R-1} : n_0 \in [R, p-1] \right\}$$

generates G. Assume therefore $R = 6$. Thus, $5D \le C$ and $6D > C$. Consider the binomial coefficient $b = \binom{10Cp^e+4C}{10Dp^e+4D}$. We obtain

$$\begin{aligned}
[10Cp^e + 4C]_p &= 12(p-1)^{e-1}0(p-1)^{e-1}3, \\
[10Dp^e + 4D]_p &= 1w_1 0 w_2 0,
\end{aligned}$$

where w_1, w_2 are of length $e-1$ with $1w_1 0 = [10D]_p$ and $w_2 0 = [4D]_p$. By Lucas' theorem we have

$$b \equiv \binom{1}{0}\binom{2}{1}\binom{p^{e-1}-1}{(1/p)(10D-p^e)}\binom{0}{0}\binom{p^{e-1}-1}{4D/p}\binom{3}{0} \pmod{p}.$$

Note that for every $c \in [0, p^{e-1}-1]$ we have $\binom{p^{e-1}-1}{c} \equiv (-1)^c \pmod{p}$. Since $4D/p$ is even and $(1/p)(10D - p^e)$ is odd, we obtain $b \equiv -2 \pmod{p}$, which is a generator of $(\mathbb{Z}/7\mathbb{Z})^\times$. ∎

LEMMA 23. *Assume that* $\lceil 2p/3\rceil + 1 < R \le \lceil 2p/3\rceil p^{v-1} + 1$. *Then* $\binom{Cn}{Dn}$ *is* p-*solvable for every prime* $p \ge 7$.

Proof. Observe that our assumptions imply $v > 1$, and thus $R + k < p^v$ for each $k \in [0, p-1]$. Hence, $[(R+k)C]_p = wa(p-1)^{e-v}w_1$, where w_1 is a word with $l(w_1) = v$ and a is a digit with $a \equiv R + k - 1 \pmod p$. Take an integer k in the interval $I = [0, \lceil 2p/3\rceil]$. Since $R > \lceil 2p/3\rceil + 1$, and so $k < R - 1$, the most significant digit of $(R+k)D$ is 1. Thus, $[(R+k)D]_p = 1w'0^v$ for some word w' of length $e - v$. Lucas' theorem implies that

$$\binom{(R+k)C}{(R+k)D} \equiv \binom{a}{1} \cdot \binom{p^e - 1}{(R+k)D - p^e} \pmod p.$$

Since $\binom{p^e-1}{c} \equiv (-1)^c \pmod p$ for $c \le p^e - 1$, we conclude that

$$\binom{(R+k)C}{(R+k)D} \equiv (-1)^{(R+k)D-p^e} a \equiv (-1)^{RD-1+kD}(R+k-1) \pmod p$$

belongs to G for every $k \in I$, with one possible exception in case $a = 0$.

If D is even, then those values are distinct and so $\#(G) > (p-1)/2$, which implies that $G = (\mathbb{Z}/p\mathbb{Z})^\times$. Assume that D is odd. Take $t = RD - 1$, and let d denote the residue of $R - 1$ modulo p. We have

$$(3) \qquad (-1)^{t+k}(d+k) \in G \cup \{0\}, \qquad k \in I.$$

If $p \in \{7, 11, 13, 17, 19\}$, then one can easily check that the nonzero values in (3) generate $(\mathbb{Z}/p\mathbb{Z})^\times$ for each $t \in \{0,1\}$ and $d \in \mathbb{Z}/p\mathbb{Z}$. Assume therefore that $p \ge 23$, and assume to the contrary that $G \ne (\mathbb{Z}/p\mathbb{Z})^\times$. Since $\#(I) > (p+1)/2$, it follows that $\{d + k : k \in I\} \setminus \{0\}$ generates G. This implies that $-1 \notin G$ and G is a subgroup of index 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$ (i.e., G is the group of nonzero quadratic residues modulo p). If $d > \lceil p/3\rceil$, then, taking $k_0 = p - 1 - d$, $k_1 = p + 1 - d$, we obtain

$$\{(-1)^{t+k_i}(d+k_i) \pmod p : i = 0, 1\} = \{1, p-1\}.$$

This contradicts the fact that $-1 \notin G$. Assume therefore $0 \le d \le \lceil p/3\rceil$. Take an even number $a \in [0, 8]$ such that $a \equiv 2p \pmod 5$. Put

$$n_0 = \frac{2p - a}{5}, \qquad n_1 = \frac{2p + 4a}{5}.$$

Since $p \ge 23$, we get $n_0, n_1 \in [\lceil p/3\rceil, \lceil 2p/3\rceil]$. Thus, $n_0, n_1 \in \{d + k : k \in I\}$. Recall that $n_1 - n_0 = a$ is even. Using (3) we obtain $(-1)^t n_0, (-1)^t n_1 \in G$ for some t. In particular, $n_0/n_1 \in G$. Since

$$\frac{n_0}{n_1} = \frac{2p + 4a}{2p - a} \equiv -4 \pmod p$$

and $4 = 2^2 \in G$, we obtain $-1 \in G$, which is a contradiction. ∎

LEMMA 24. *Assume that* $R > \lceil 2p/3\rceil p^{v-1} + 1$. *Then* $\binom{Cn}{Dn}$ *is* p-*solvable for every prime* $p \ge 7$.

Proof. Let $t = \lceil 2p/3 \rceil$, $n_0 = tp^{v-1} + 1$ and take $n_1 = p^v + r$ for some $r \in [2, t]$. Our assumption implies that $l(Dn_0) \leq e$. Since $[Cn_0]_p = t0^{v-1}(p-1)^{e-v}w'$ for some word w' of length v, we obtain $Dn_0 \preceq Cn_0$. Write

$$[Cn_0]_p = tw_0, \quad [Dn_0]_p = z_0,$$

where w_0, z_0 are words with $l(w_0) \geq l(z_0)$. Take $a = e + 1 - l(Dn_1)$, and note that

$$[Cn_1]_p = 10^{v-1}(r-1)(p-1)^{e-v-1}(p-2)(p-1)^{v-1}(p-r), \quad 0^a[Dn_1]_p = bw0^v,$$

where $l(w) = e - v$ and $b \in \{0, 1, 2\}$. Note that the case $b = 2$ is possible only when $v = 1$. Moreover, it implies that $n_1 \geq 2R - 1$ and so $p + r \geq 2R - 1 \geq 2\lceil 2p/3 \rceil + 3$, which gives $r \geq 3$. Thus, $b \leq r - 1$. Let s denote the least significant digit of w. Assuming $s \neq p - 1$, we obtain $Dn_1 \preceq Cn_1$. Write

$$[Cn_1]_p = w_1(p-2)(p-1)^{v-1}(p-r), \quad [Dn_1]_p = z_1 s 0^v.$$

Take $n = p^{l(Cn_0)-1}n_1 + n_0$. Since $p - r + t \geq p$, we obtain

$$[Cn]_p = w_1(p-1)0^{v-1}(t-r)w_0, \quad [Dn]_p = z_1 s 0^{l(w_0)-l(z_0)+v} z_0.$$

Lucas' theorem gives

$$\frac{\binom{Cn_0}{Dn_0}\binom{Cn_1}{Dn_1}}{\binom{Cn}{Dn}} \equiv \frac{\binom{p-2}{s}}{\binom{p-1}{s}} \pmod{p}.$$

Thus, $s + 1 = \binom{p-2}{s}/\binom{p-1}{s} \in G$. Denote by $d \in (\mathbb{Z}/p\mathbb{Z})^\times$ the residue of D/p^v modulo p. We have $s \equiv dr \pmod{p}$. Thus, $dr + 1 \in G$ for every $r \in [2, t] \setminus \{-1/d\}$. If $p \geq 11$, this implies $\#(G) > (p-1)/2$, and so $G = (\mathbb{Z}/p\mathbb{Z})^\times$. For $p = 7$, it can be easily checked that the set $S_d = \{dr + 1 : r \in [2, t] \setminus \{-1/d\}\}$ generates G for each $1 \leq d \leq 6$. ∎

Lemmas 22–24 prove Theorem 1 in the cases $D \equiv 0, C \pmod{p}$.

3.3. Proofs of Corollaries 2 and 3. Recall that, apart from the cases $D \equiv 0, C/2, C \pmod{p}$, we have proved Theorem 1 for the prime 5 also.

Proof of Corollary 2. If $(C, D, p) \neq (2, 1, 3), (2, 1, 5)$, then this is a direct consequence of Theorem 1. In the cases $(C, D, p) = (2, 1, 3), (2, 1, 5)$, we infer that $2 = \binom{2}{1} \in G$ is a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$. ∎

Proof of Corollary 3. If $C \not\equiv 1, 2 \pmod{p}$ or $p > 5$, then this is a direct consequence of Theorem 1. If $p = 2$, then it follows from Lemmas 10 and 11. For the cases $C \equiv 2 \pmod{p}$ and $p = 3, 5$, note that $\binom{C}{1} \equiv 2 \pmod{p}$ is a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$.

Assume therefore $C \equiv 1 \pmod{p}$ and $p = 3, 5$. Take $n_0 = 1$ and let $n_1 < p$ be such that the most significant digit of Cn_1 is 1. Lemma 12 shows that

$2 = \binom{1+1}{1+0}/\binom{1}{1}\binom{1}{0} \in G$. Since 2 is a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$ for $p = 3, 5$, this implies the corollary. ∎

4. WEAK WELL-DISTRIBUTION

In this section we prove Lemma 5 and Theorems 6 and 8. It turns out to be convenient to begin with Theorem 8 and to use it to obtain Lemma 5 and Theorem 6.

4.1. Proof of Theorem 8(i)–(iii). One can easily prove the following two lemmas (cf. [15, Lemma 11, Proposition 22]).

LEMMA 25. *Let $X \subseteq \mathbb{N}$ and $0 \le \alpha \le 1$. Assume that*

$$\max_{j\ge 1}\left|\frac{\#(X\cap[jp^l,(j+1)p^l))}{p^l}-\alpha\right| \xrightarrow[l\to\infty]{} 0.$$

Then X is of Banach density α.

LEMMA 26. *Let $P_w(l)$ denote the probability that a random word z, chosen uniformly from $(\mathbb{Z}/p\mathbb{Z})^l$, does not contain w as a subword. Then*

$$\lim_{l\to\infty} P_w(l) = 0.$$

In fact, we will prove (Lemma 33) a more general version of Lemma 26. (We will also prove (Lemma 29) a claim which is very similar to Lemma 25.)

LEMMA 27. *Let w be a word over $\mathbb{Z}/p\mathbb{Z}$. Denote by X the set of numbers $n \in \mathbb{N}$ such that $[n]_p$ does not contain w as a subword. Then $BD(X) = 0$.*

Proof. Let $j, l \ge 1$ and choose uniformly at random an integer n in the interval $[jp^l, (j+1)p^l)$. Note that $[n]_p = [j]_p z$ where z is a random word of length l. Thus, the probability that $[n]_p$ does not contain w as a subword is $\le P_w(l)$ and the lemma follows from Lemmas 25 and 26. ∎

Let $A_n = \left(\binom{C_1 n}{D_1 n}, \binom{C_2 n}{D_2 n}, \ldots, \binom{C_m n}{D_m n}\right)$ and G be as in Theorem 8. Put $L = \max_{i=1}^m l(C_i)$. The following lemma is a direct consequence of Lemma 9.

LEMMA 28. *Let $n, n_0, n_1 > 0$ be integers and assume that $[n]_p = [n_0]_p 0^l [n_1]_p$ for some $l \ge L$. Then*

$$A_n \equiv A_{n_0} A_{n_1} \pmod{p}.$$

Proof of the first three parts in Theorem 8. (i) Lemma 28 implies that G is a group.

(ii) follows by observing that $A_{p^i n} \equiv A_n \pmod p$ for each i and n.

(iii) Note that the set in question is a subset of

$$X = \left\{ n \in \mathbb{N} : \binom{C_1 n}{D_1 n} \not\equiv 0 \pmod{p} \right\}.$$

Thus, it suffices to prove that $BD(X) = 0$. By Lemma 11 there exists an n' with $\binom{C_1 n'}{D_1 n'} \equiv 0 \pmod{p}$. Put $w = 0^{l_1}[n']_p 0^{l_1}$, where $l_1 = l(C_1)$. Lemma 9 implies that for each integer $n > 0$ whose base p representation contains the word w we have $\binom{C_1 n}{D_1 n} \equiv 0 \pmod{p}$ and so $n \notin X$. Thus, the assertion follows from Lemma 27. ∎

4.2. Proof of Theorem 8(iv). Take $r \in G$ and let $X_r = \{n \in \mathbb{N} : A'_n = r\}$. For every $j, l \geq 1$ put

$$I_{j,l} = [jp^l, (j+1)p^l), \qquad I'_{j,l} = \{n \in I_{j,l} : A_n \in ((\mathbb{Z}/p\mathbb{Z})^\times)^m \pmod{p}\}.$$

Denote by $\mathcal{N}_l$ the set of numbers $j \geq 1$ such that $I'_{j,l} \neq \emptyset$.

Let us first sketch the proof: We start by showing (Lemma 29) that, in order to prove that $BD(X_r) = 1/\#(G)$, it is enough to consider the distribution of $(A_n \pmod{p})_{n \in I}$ on the sets $I = I'_{j,l}$ with large l's. Then we define a partition $\mathcal{P}$ of $I'_{j,l}$ such that the size of each $Y \in \mathcal{P}$ is either 1 or $\#(G)$. Moreover, taking a large l, we prove that "almost every" $Y \in \mathcal{P}$ is of cardinality $\#(G)$, where $(A_n \pmod{p})_{n \in Y}$ takes each value in G exactly once. This implies that

$$\frac{\#\{n \in I'_{j,l} : A_n \equiv g \pmod{p}\}}{\#(I'_{j,l})} \approx \frac{1}{\#(G)} \quad \text{for each } g \in G.$$

Lemma 29. *Assume that*

$$\max_{j \in \mathcal{N}_l} \left| \frac{\#\{n \in I'_{j,l} : A_n \equiv r \pmod{p}\}}{\#(I'_{j,l})} - \frac{1}{\#(G)} \right| \xrightarrow[l \to \infty]{} 0. \tag{4}$$

Then $BD(X_r) = 1/\#(G)$.

Proof. Let M be a (large) positive integer. Take an interval $I = [a, b)$ such that $I' = \{n \in I : A_n \in ((\mathbb{Z}/p\mathbb{Z})^\times)^m \pmod{p}\}$ contains at least M elements. Put $l = \lfloor l(M)/2 \rfloor$ and consider the sets $I'_{j,l}$ for integers j in $[a/p^l, b/p^l - 1]$. Note that those $I'_{j,l}$ are disjoint subsets of I'. If M (and hence l) is large, most of the elements of I' belong to some $I'_{j,l}$ with j in $[a/p^l, b/p^l - 1]$. In fact, we have

$$\frac{\#(I') - \sum_{j=\lceil a/p^l \rceil}^{\lfloor b/p^l \rfloor - 1} \#(I'_{j,l})}{\#(I')} \leq \frac{2p^l}{M} = \frac{2p^{\lfloor l(M)/2 \rfloor}}{M} \xrightarrow[M \to \infty]{} 0.$$

Let $\varepsilon > 0$. If M (and hence l) is large, then (4) implies that

$$\left| \frac{\#\{n \in I'_{j,l} : A_n \equiv r \pmod{p}\}}{\#(I'_{j,l})} - \frac{1}{\#(G)} \right| < \varepsilon$$

for every $j \in \mathcal{N}_l$. Thus, for large enough M we have

$$\left| \frac{\#\{n \in I' : A_n \equiv r \pmod{p}\}}{\#(I')} - \frac{1}{\#(G)} \right| < \varepsilon$$

for every set I' of the form $I' = \{n \in [a,b) : A_n \in ((\mathbb{Z}/p\mathbb{Z})^\times)^m \pmod{p}\}$ of size $\#(I') \geq M$. ∎

LEMMA 30. *There exist $\#(G)$ integers $(R_g)_{g \in G}$ such that*

(i) $A_{R_g} \equiv g \pmod{p}$ *for each $g \in G$.*
(ii) *The base p representations $([R_g]_p)_{g \in G}$ are of the same length, and end with a nonzero digit.*

Proof. For each $g \in G$ take a positive integer n_g such that $A_{n_g} \equiv g \pmod{p}$. Since $A_{p^i n} \equiv A_n \pmod{p}$ for each i, we may assume that each n_g is prime to p and so $[n_g]_p$ ends with a nonzero digit.

Put $l = \max_{g \in G} l(n_g)$. For each $g \in G$ let R_g be the integer whose base p representation contains $\#(G)+1$ occurrences of $[n_g]_p$ which are separated by blocks of 0's as follows:

$$[R_g]_p = ([n_g]_p 0^L)^{\#(G)} 0^{(\#(G)+1)(l - l(n_g))} [n_g]_p.$$

Obviously, $l(R_g) = (\#(G)+1)l + \#(G)L$. By Lemma 28,

$$A_{R_g} \equiv (A_{n_g})^{\#(G)+1} \equiv A_{n_g} \equiv g \pmod{p}. \ ∎$$

Let $(R_g)_{g \in G}$ be as in Lemma 30 and $L_0 = l(R_g)$ be the length of the base p representation of each R_g. For every $g \in G$ let $s_g = 0^{L_0}[R_g]_p 0^{L_0}$. Put

$$\mathcal{G} = \{s_g : g \in G\}.$$

Let $j, l \geq 1$. Consider the bijection ω between $I_{j,l}$ and the set of words $w \in (\mathbb{Z}/p\mathbb{Z})^l$, where $\omega(n)$ is the (unique) word satisfying $[n]_p = [j]_p \omega(n)$. Take $n \in I_{j,l}$. Assume that $\omega(n)$ contains one of the words in $\mathcal{G}$ and write $\omega(n) = w' s w''$ with $s \in \mathcal{G}$ and w'' as short as possible. The *$\mathcal{G}$-class* $\mathcal{X}_n = \mathcal{X}_n(l,j)$ of n is the following subset of $I_{j,l}$:

$$\mathcal{X}_n = \{k \in I_{j,l} : \omega(k) \in w' \mathcal{G} w''\} \tag{5}$$

(where we write $w'\mathcal{G}w''$ for the set $\{w' s_g w'' : s_g \in \mathcal{G}\}$). If $\omega(n)$ contains none of the words of $\mathcal{G}$, then the $\mathcal{G}$-class of n is $\mathcal{X}_n = \{n\}$ and called *trivial*. Note that every nontrivial $\mathcal{G}$-class is of cardinality $\#(G)$. Put

$$\mathcal{P} \ (= \mathcal{P}(j,l)) = \{\mathcal{X}_n : n \in I'_{j,l}\}.$$

LEMMA 31. *For every nontrivial $\mathcal{G}$-class $\mathcal{X}_n \in \mathcal{P}(j,l)$ and $g \in G$, we have $A_k \equiv g \pmod{p}$ for exactly one element $k \in \mathcal{X}_n$.*

Proof. Write $\omega(n) = w' s_g w''$ where $s_g \in \mathcal{G}$ and w'' is as short as possible. Let t be the integer whose base p representation is $[t]_p = [j]_p w' 0^L w''$. The definition of $\mathcal{X}_n$ and Lemma 28 imply that the elements in $\{A_k : k \in \mathcal{X}_n\}$ are congruent to $\{A_t g : g \in G\}$ modulo p. This implies the lemma. ∎

Lemma 32. *$\mathcal{P}$ is a partition of $I'_{j,l}$.*

Proof. Since each $[R_g]_p$ begins and ends with a nonzero letter, we easily see that any two $\mathcal{G}$-classes are either equal or disjoint. Since $n \in \mathcal{X}_n$, we have $I'_{j,l} \subseteq \bigcup \mathcal{P}$. Lemma 31 shows that for each $\mathcal{X}_n \in \mathcal{P}$ we have $\{A_k \bmod p : k \in \mathcal{X}_n\} \subseteq ((\mathbb{Z}/p\mathbb{Z})^\times)^m$ and so $\mathcal{X}_n \subseteq I'_{j,l}$. Thus, $\bigcup \mathcal{P} = I'_{j,l}$. ■

Our next goal is to prove (taking a "large" l) that for most numbers $n \in I'_{j,l}$ we have $[n]_p = [j]_p w$ for some word $w \in (\mathbb{Z}/p\mathbb{Z})^l$ containing a subword $s \in \mathcal{G}$. (See Proposition 39 for the precise formulation.) This will show that most of the $\mathcal{G}$-classes $Y \in \mathcal{P}$ are of cardinality $\#(Y) = \#(G)$. We will relate this problem to a walk on a certain graph Γ_0 whose paths correspond to subwords in base p representations of elements in $I'_{j,l}$. Therefore we introduce some terminology from graph theory:

Definition. A directed (multi)graph $\Gamma = (V, E)$ is *strongly connected* if, for every pair (u, v) of vertices, there exists a directed path from u to v. Γ is a *primitive graph* (cf. [10]) if there exists a $K > 0$ such that, for every $l \ge K$ and $u, v \in V$, there exists a path from u to v of length l. This is equivalent to the property that some power of the adjacency matrix M_Γ is strictly positive (i.e., M_Γ is a *primitive matrix*).

The property of primitive graphs that we need is the following

Lemma 33. *Let $\Gamma = (V, E)$ be a directed primitive multigraph, $u, v \in V$ and P be a directed path in Γ. For every $l \ge 0$, let $N_{u,v}(l)$ denote the number of paths of length l from u to v, and $N^P_{u,v}(l)$ the number of those paths which contain P as a subpath. Then*

$$\lim_{l\to\infty} \frac{N^P_{u,v}(l)}{N_{u,v}(l)} = 1.$$

Proof. Since Γ is primitive, there exists a K such that $N^P_{u,v}(l) \ge 1$ for every $u, v \in V$ and $l \ge K$. Take $l \ge K$, and decompose the interval $I = [0, l)$ into a disjoint union of $t = \lfloor l/K \rfloor$ subintervals $\Delta_i = [\delta_i, \delta_{i+1})$ where $\delta_i = Ki$ for $i \in [0, t)$ and $\delta_t = l$. Thus, $K \le \#(\Delta_i) \le 2K$ for every i. For each sequence $a_0 a_1 \ldots a_t$ of length $t+1$ over V, let $\mathcal{M}_{a_0,\ldots,a_t}$ denote the number of paths of length l from a_0 to a_t which visit a_i at the δ_ith step ($i \le t$). Let $\mathcal{M}^{\bar{P}}_{a_0,\ldots,a_t}$ denote the number of those paths which do not contain P as a subpath. Since $\delta_{i+1} - \delta_i \ge K$, we have $N^P_{a_i,a_{i+1}}(\delta_{i+1} - \delta_i) \ge 1$. Thus,

$$\frac{\mathcal{M}^{\bar{P}}_{a_0,\ldots,a_t}}{\mathcal{M}_{a_0,\ldots,a_t}} \le \frac{\prod_{i=0}^{t-1}(N_{a_i,a_{i+1}}(\delta_{i+1} - \delta_i) - 1)}{\prod_{i=0}^{t-1} N_{a_i,a_{i+1}}(\delta_{i+1} - \delta_i)} \le \left(1 - \frac{1}{M}\right)^t,$$

where $M = \max\{N_{u,v}(l) : u, v \in V,\ l \le 2K\}$. This implies

$$\frac{N_{a_0,a_t}(l) - N^P_{a_0,a_t}(l)}{N_{a_0,a_t}(l)} \le \left(1 - \frac{1}{M}\right)^t.$$

Since $t = \lfloor l/K \rfloor \to \infty$ as $l \to \infty$, we obtain

$$\lim_{l\to\infty} \frac{N_{a_0,a_t}(l) - N^P_{a_0,a_t}(l)}{N_{a_0,a_t}(l)} = 0. \ \blacksquare$$

Remark. Lemma 26 can be considered as a special case of Lemma 33 by taking Γ to be the complete directed graph on the vertex set $\mathbb{Z}/p\mathbb{Z}$.

Let $n, k, i \ge 0$. We write $k \preceq_i n$ if the ith digit of k does not exceed the ith digit of n. (Thus, $k \preceq n$ if $k \preceq_i n$ for each i.) Given a word $w = n_{l-1} \dots n_0$ over $\mathbb{Z}/p\mathbb{Z}$, put $n_w = \sum_{i=0}^{l-1} n_i p^i$. For each $t \in \{1, \dots, m\}$, let f_t be the function from the set of all words over $(\mathbb{Z}/p\mathbb{Z})$ to $\mathbb{N}^2$ given by

$$f_t(w) = \left(\left\lfloor \frac{C_t n_w}{p^{l(w)}} \right\rfloor, \left\lfloor \frac{D_t n_w}{p^{l(w)}} \right\rfloor \right).$$

That is, $f_t(w) = (c, d)$ if $[C_t n_w]_p = [c]_p z_0$ and $[D_t n_w]_p = [d]_p z_1$ for some words z_0, z_1 of length $l = l(w)$ (where we put $c = 0$ if $l(C_t n_w) \le l(w)$ and $d = 0$ if $l(D_t n_w) \le l(w)$). Note that $C_t n_w / p^{l(w)} < C_t$ and thus $\mathrm{Im}(f_t) \subseteq [0, C_t)^2$ is finite.

Lemma 34. *Let z, w be words over $\mathbb{Z}/p\mathbb{Z}$ and $(c, d) = f_t(w)$. Then*

$$f_t(zw) = \left(\left\lfloor \frac{c + C_t n_z}{p^{l(z)}} \right\rfloor, \left\lfloor \frac{d + D_t n_z}{p^{l(z)}} \right\rfloor \right).$$

In particular, for any words w_1, w_2 over $\mathbb{Z}/p\mathbb{Z}$ with $f_t(w_1) = f_t(w_2)$ we have $f_t(zw_1) = f_t(zw_2)$.

Proof. The definition of f_t yields $C_t n_w = cp^{l(w)} + q_1$ and $D_t n_w = dp^{l(w)} + q_2$ for some $q_1, q_2 < p^{l(w)}$. Thus,

$$C_t(n_z p^{l(w)} + n_w) = (c + C_t n_z) p^{l(w)} + q_1,$$
$$D_t(n_z p^{l(w)} + n_w) = (d + D_t n_z) p^{l(w)} + q_2,$$

which implies the lemma. $\blacksquare$

Put

$$f(w) = (f_1(w), \dots, f_m(w)),$$

and for every $v = f(w) \in \mathrm{Im}(f)$ and $a \in \mathbb{Z}/p\mathbb{Z}$ let $v_a = f(aw)$. Note that, by Lemma 34, v_a depends only on v, a (and not on w), and thus it is well defined.

Define a directed multigraph Γ whose set of vertices is $V = \mathrm{Im}(f)$. Let $v = ((c_1, d_1), \dots, (c_m, d_m))$ be an element in V. For every $a \in \mathbb{Z}/p\mathbb{Z}$ such that $d_t + D_t a \preceq_0 c_t + C_t a$ for each $t \le m$, we put a directed edge (called an *a-edge*) from v to v_a. It may happen that $v_a = v_b$ for distinct $a, b \in \mathbb{Z}/p\mathbb{Z}$ and thus we may have multiedges (with different labeling) in Γ. Our definitions yield

LEMMA 35. *Let $v = f(w) \in \mathrm{Im}(f)$. Then (v, v_a) is an a-edge in Γ if and only if*

$$D_t n_{aw} \preceq_{l(w)} C_t n_{aw}, \qquad t = 1, \ldots, m. \tag{6}$$

Note that (6) implies that $D_t n_{zaw} \preceq_{l(w)} C_t n_{zaw}$ for any word z.

Let $z = a_{l-1} \ldots a_0 \in (\mathbb{Z}/p\mathbb{Z})^l$. A directed path P of length l in Γ is a *z-path* if the ith edge in P is an a_i-edge for $i \le l-1$.

Let V_0 denote the *strongly connected component* of $f(\Lambda) = (0,0)^m \in V$ in Γ. That is, V_0 consists of those vertices v for which there is a closed path containing both v and $(0,0)^m$. Let $\Gamma_0 = (V_0, E_0)$ be the graph on the vertices V_0 induced by Γ. A vertex $((c_1, d_1), \ldots, (c_m, d_m)) \in V$ is *admissible* if $d_t \preceq c_t$ for each $t \le m$.

LEMMA 36.

(i) *A vertex $v \in V$ is admissible if and only if there exists a 0^l-path in Γ from v to $(0,0)^m$ for some l.*
(ii) *Let $n \ge 0$ be an integer. Then $A_n \in ((\mathbb{Z}/p\mathbb{Z})^\times)^m \pmod p$ if and only if there is an $[n]_p$-path P in Γ_0 from $(0,0)^m$ to an admissible vertex.*

Proof. (i) follows directly from the definition of the 0-edges in Γ.

(ii) Assume that $A_n \in ((\mathbb{Z}/p\mathbb{Z})^\times)^m \pmod p$ and let $[n]_p = n_{l-1} \ldots n_0$. Then $D_t n \preceq C_t n$ for each $t \le m$, so that

$$f(\Lambda) = (0,0)^m, f(n_0), f(n_1 n_0), f(n_2 n_1 n_0), \ldots, f([n]_p)$$

is an $[n]_p$-path in Γ from $(0,0)^m$ to an admissible vertex. By (i), there is a path from $f([n]_p)$ to $(0,0)^m$. Thus the above path is also contained in the graph Γ_0.

Assume now that there is an $[n]_p$-path P in Γ_0 from $(0,0)^m$ to an admissible vertex. The definition of the edges in Γ implies that each digit of $D_t n$ does not exceed the corresponding digit of $C_t n$ for each t. Hence $\binom{C_t n}{D_t n} \not\equiv 0 \pmod p$. ∎

LEMMA 37. *For every $s \in \mathcal{G}$ there exists an s-path in Γ_0.*

Proof. Write $s = 0^{L_0}[R_g]_p 0^{L_0}$ and put $s' = [R_g]_p 0^{L_0}$, $n = n_s$ $(= n_{s'})$. Recall that $A_n \equiv g \pmod p$. Thus, by Lemma 36(ii), there is an s'-path in Γ_0 from $(0,0)^m$ to an admissible vertex v. This implies that for each $a \ge 0$ there is a $0^a s'$-path in Γ_0 starting at $(0,0)^m$. ∎

LEMMA 38. *The graph Γ_0 is primitive.*

Proof. Γ_0 is a strongly connected graph by its definition. Since it contains a loop (over the vertex $(0,0)^m$), it is primitive. ∎

PROPOSITION 39. *Let* $\mathcal{X}_n(j,l)$ *be as in* (5). *Then*

$$\max_{j\in\mathcal{N}_l} \frac{\#(n \in I'_{j,l} : \mathcal{X}_n(j,l) = \{n\})}{\#(I'_{j,l})} \xrightarrow[l\to\infty]{} 0.$$

Proof. Take $l \geq 1$ and $j \in \mathcal{N}_l$. Denote by V_j the set of vertices v such that there is a $[j]_p$-path in Γ_0 from v to an admissible vertex. Let $w \in (\mathbb{Z}/p\mathbb{Z})^l$. Lemma 36(ii) implies that $jp^l + n_w \in I'_{j,l}$ if and only if there is a w-path in Γ_0 from $(0,0)^m$ to a vertex in V_j. If we take l large, we deduce from Lemmas 33, 37, 38 that most of the paths of length l from $(0,0)^m$ to a vertex in V_j contain an s-path for some $s \in \mathcal{G}$. This implies that, for most of the elements $n \in I'_{j,l}$, we have $[n]_p = [j]_p w$ for some word $w \in (\mathbb{Z}/p\mathbb{Z})^l$ which contains a subword $s \in \mathcal{G}$ (and so $\mathcal{X}_n(j,l)$ is of cardinality $\#(G)$). ∎

Proof of Theorem 8(iv). Lemma 31 and Proposition 39 show that

$$\max_{j\in\mathcal{N}_l} \left| \frac{\#\{n \in I'_{j,l} : A_n \equiv r \ (\mathrm{mod}\, p)\}}{\#(I'_{j,l})} - \frac{1}{\#(G)} \right| \xrightarrow[l\to\infty]{} 0.$$

Thus the theorem follows from Lemma 29. ∎

REMARK. Let $\mathcal{L}$ denote the set of all words w over $\Omega = \mathbb{Z}/p\mathbb{Z}$ such that $A_{n_w} \in ((\mathbb{Z}/p\mathbb{Z})^\times)^m \ (\mathrm{mod}\, p)$. Our construction of Γ_0 implies that $\mathcal{L}$ is a regular language. In fact, let $\mathcal{A}$ be the automaton on the state set $Q = V_0$ which is given by the graph Γ_0, taking $(0,0)^m$ as the starting state and the admissible vertices as the final states. Lemma 36(ii) shows that $\mathcal{L}$ is the language which is accepted by $\mathcal{A}$ (when we agree that $\mathcal{A}$ reads words w from right to left). In particular, the binary sequence $(b_n)_{n=0}^\infty$, obtained from (A_n) by putting $b_n = 1$ if $A_n \in ((\mathbb{Z}/p\mathbb{Z})^\times)^m \ (\mathrm{mod}\, p)$, is an automatic sequence. We refer the reader to [2] for an excellent book on automatic sequences.

4.3. Multinomial coefficients. In this subsection $A_n = \binom{Kn}{K_1 n, \ldots, K_m n}$ where $K_1, \ldots, K_m$ are positive integers whose sum is K. Let $G_A \subseteq (\mathbb{Z}/p\mathbb{Z})^\times$ be the set of nonzero residues modulo p which are visited by $(A_n \bmod p)_{n=1}^\infty$. Note that each A_n can be represented as a product of binomial coefficients:

$$A_n = \binom{Kn}{K_1 n} \binom{(K-K_1)n}{K_2 n} \binom{(K-K_1-K_2)n}{K_3 n} \cdots \binom{(K_{m-1}+K_m)n}{K_{m-1} n}.$$

Let B_n be the sequence in $(\mathbb{Z}/p\mathbb{Z})^{m-1}$ given by

$$B_n = \left(\binom{Kn}{K_1 n}, \binom{(K-K_1)n}{K_2 n}, \binom{(K-K_1-K_2)n}{K_3 n}, \ldots, \binom{(K_{m-1}+K_m)n}{K_{m-1} n} \right),$$

and G_B be the corresponding subgroup of $((\mathbb{Z}/p\mathbb{Z})^{\times})^{m-1}$ given in Theorem 8(i). Define the function $\varphi : (\mathbb{Z}/p\mathbb{Z})^{m-1} \to \mathbb{Z}/p\mathbb{Z}$ by

$$\varphi(a_1, \ldots, a_{m-1}) = \prod_{i=1}^{m-1} a_i.$$

Since $A_n = \varphi(B_n)$, we easily obtain Lemma 5 from the first three parts of Theorem 8. In particular, G_A is a group.

Proof of Theorem 6. Note that φ induces a homomorphism from G_B onto G_A. Let $r \in G_A$. There are exactly $\#(G_B)/\#(G_A)$ elements $r' \in G_B$ with $\varphi(r') = r$. Since each of them is visited by the sequence B'_n with the same (Banach) frequency $1/\#(G_B)$, we conclude that

$$BD(\{n \in \mathbb{N} : A'_n \equiv r \pmod{p}\}) = \frac{\#(G_B)}{\#(G_A)} \cdot \frac{1}{\#(G_B)} = \frac{1}{\#(G_A)}. \ \blacksquare$$

Acknowledgments. The author is grateful to Daniel Berend for introduction to the subject and valuable discussions and to the anonymous referees for helpful suggestions.

References

[1] J.-P. Allouche et V. Berthé, *Triangle de Pascal, complexité et automates*, Bull. Belg. Math. Soc. 4 (1997), 1–23.

[2] J.-P. Allouche and J. Shallit, *Automatic Sequences. Theory, Applications, Generalizations*, Cambridge Univ. Press, Cambridge, 2003.

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

[4] D. Berend and J. E. Harmse, *On some arithmetical properties of middle binomial coefficients*, Acta Arith. 84 (1998), 31–41.

[5] N. J. Fine, *Binomial coefficients modulo a prime*, Amer. Math. Monthly 54 (1947), 589–592.

[6] H. Furstenberg, *Recurrence in Ergodic Theory and Combinatorial Number Theory*, Princeton Univ. Press, 1981.

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

[8] J. W. L. Glaisher, *On the residue of a binomial-theorem coefficient with respect to a prime modulus*, Quart. J. Pure Appl. Math. 30 (1899), 150–156.

[9] A. Granville, *Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers*, in: Organic Mathematics (Burnaby, BC, 1995), CMS Conf. Proc. 20, Amer. Math. Soc., Providence, RI, 1997, 253–276.

[10] G. Jones, M. Klin and Y. Moshe, *Primitivity of permutation groups, coherent algebras and matrices*, J. Combin. Theory Ser. A 98 (2002), 210–217.

[11] N. Kriger, *Arithmetical properties of some sequences of binomial coefficients*, M. Sc. thesis, Ben-Gurion Univ., 2001.

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

[13] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl. 20, Addison-Wesley, 1983.
[14] É. Lucas, *Sur les congruences des nombres eulériens et les coefficients différentiels des fonctions trigonométriques suivant un module premier*, Bull. Soc. Math. France 6 (1878), 49–54.
[15] Y. Moshe, *On a problem of Granville and Zhu regarding Pascal's triangle*, Mathematika 51 (2005), 63–82.
[16] W. Narkiewicz, *Uniform Distribution of Sequences of Integers in Residue Classes*, Lecture Note in Math. 1087, Springer, Berlin, 1984.
[17] H. Schwerdtfeger, *Geometry of Complex Numbers*, Math. Expositions 13, Univ. of Toronto Press, Toronto, 1962.

Einstein Institute of Mathematics
Edmond J. Safra Campus, Givat Ram
The Hebrew University of Jerusalem
Jerusalem, 91904, Israel
E-mail: moshey@math.bgu.ac.il

Received on 10.4.2006
and in revised form on 7.1.2007 (5179)