Binomial Coefficients as Functions of their Denominator; Another Primality Criteria for Natural Integers

Nikita Gogin and Vladislav Shubin

Abstract. We prove that an odd positive integer n is prime iff denominator of the rational number $\langle\binom{n}{n-1}\rangle$ is n^{n-1}, where $\langle\binom{n}{x}\rangle = \mathcal{B}_n(x)$ is interpolation polynomial on x for the set of binomial coefficients $\{\binom{n}{r}\}_{r=0,1,\ldots,n}$ and $x \in [0,n] \subset \mathbb{R}$.

Keywords. Prime numbers, Binomial coefficients, Interpolation polynomial, Newton interpolation formula, Krawtchouk polynomials.

1. Introduction and Preliminaries

Binomial coefficients have
surprisingly great expressive power ...
Yu. V. Matiyasevich [2]

In this paper we use generally accepted definition of the (generalized) binomial coefficients as polynomials on the (real) variable x:

$$\binom{x}{m} = \frac{x(x-1)\ldots(x-m+1)}{m!} \tag{1}$$

where m is a nonnegative integer, $\binom{x}{0} = 1$. [3]
However in joint publication [4], among other things, we proved that the identity

$$\binom{n}{k} = (-2)^n \sum_{i=0}^{n} \binom{\frac{i-1}{2}}{n} K_i^{(n)}(k) \tag{2}$$

is valid for all integer $k, 0 \leq k \leq n$, where $K_i^{(n)}(k)$ are the Krawtchouk polynomials of order n. [3]

The right side of this equality is a polynomial on k and this allows us to accept it as the definition of the symbol $\langle\binom{n}{x}\rangle$ where x stands for k and can be treated now as an element of any (not necessarily commutative) algebra over a field of zero characteristic and n is a (fixed) nonnegative integer. In particular if $x \in [0, n] \subset \mathbb{R}$ the polynomial $\mathcal{B}_n(x) = \langle \binom{n}{x} \rangle$ is of course the ordinal interpolation polynomial for the set of binomial coefficients $\{\binom{n}{r}\}_{r=0,1,\ldots,n}$. expanded by the (orthogonal) basis of Krawtchouk polynomials. Since $\mathcal{B}_n(x)$ is interpolation polynomial, we can use its notation in any form convenient for our purposes. Here we take the explicit Newton interpolation formula for equidistant nodes with a step $h = 1$ [5]:

Let $f(k), k = 0, 1, \ldots, n$ be a tuple of values of a real function f. Then the following formula for interpolation polynomial $P_n(f; x)$ is s valid:

$$P_n(f; x) = \sum_{m=0}^{n} \binom{x}{m} \sum_{k=0}^{m} (-1)^{m-k} \binom{m}{k} f(k), \tag{3}$$

where $x \in [0, n] \subset \mathbb{R}$.

2. Some Auxiliary Formulas

Applying formula (3) to $x = n^{-1}$ and $f(k) = \binom{n}{k}$ we get the equality

$$\mathcal{B}_n(n^{-1}) = \left\langle \binom{n}{n^{-1}} \right\rangle = \sum_{m=0}^{n} \binom{n^{-1}}{m} \sum_{k=0}^{m} (-1)^{m-k} \binom{m}{k} \binom{n}{k}. \tag{4}$$

Let now $A^{(n)}$ and $B^{(n)}$ be two auxiliary arrays :

$A^{(n)} = \{a_m\}_{0 \le m \le n}$, with $a_0 = 1$
and for $1 \le m \le n$

$$a_m = \binom{n^{-1}}{m} = \frac{n^{-1}(n^{-1} - 1)(n^{-1} - 2) \ldots (n^{-1} - (m-1))}{m!} = \frac{\lambda_m}{n^m}, \tag{5}$$

where

$$\lambda_m = \frac{\prod_{r=0}^{m-1} (1 - nr)}{\prod_{s=1}^{m} s}, \tag{6}$$

and

$B^{(n)} = \{b_m\}_{0 \le m \le n}$ with $b_0 = 1$ and for $1 \le m \le n$

$$b_m = \sum_{k=0}^{m} (-1)^{m-k} \binom{m}{k} \binom{n}{k} = \#_{t^m}[(1-t)^m (1+t)^{(n+m)-m}] = K_m^{(n+m)}(m). \tag{7}$$

In particular if $m = n$ and n is odd then $b_n = 0$ [6]. Formula (4) evidently can be written as a scalar product:

$$\mathcal{B}_n(n^{-1}) = \left\langle A^{(n)}, B^{(n)} \right\rangle \tag{8}$$

.

From the equalities (4),(7) and (8) we get the "duality" formula:

$$\binom{n}{n^{-1}} = \sum_{m=0}^{n} \binom{n^{-1}}{m} K_m^{(n+m)}(m). \tag{9}$$

Lemma 1. 1. (a) *If $1 < s \le m$ is an index of the denominator of formula* (6) such that gcd(s,n)=1 then there exists a unique index r , $0 \le r \le m-1$ in its numerator such that $s|(1-nr)$;

(b) In particular if $n = p$ is an odd **prime** integer then all numbers λ_m are **integers** with $\gcd(\lambda_m, n = p) = 1$ for all $m < n = p$.

2. (a) $a_n = \frac{a_{n-1}(1-n(n-1))}{n}$ *for any n;*

(b) *in particular if $n = p$ then* $\lambda_p = 1 - p(p-1) \equiv 1 \bmod (p)$*;*

3. (a) $A^{(p)} = \left\{ \{a_m = \frac{\lambda_m}{p^m}\}_{0 \le m \le (p-1)}, a_p = \frac{\lambda_{p-1}(1-p(p-1))}{p^{p+1}} \right\}$*;*

(b) *Denominators of $A^{(p)}$ are*

$$\begin{cases} p^m & \text{for } 0 \le m \le p-1 \\ p^{p+1} & \text{for } m = p \end{cases}. \tag{10}$$

Proof. 1. $s|(1-nr) \iff r = n^{-1} (\mathrm{mod}\ s)$ is unique because $\gcd(s, n) = 1$;

The special case $n = p$ is obvious from formula (5);

2. (a) is clear from formula (5);

(b) is evident;

3. is obvious from 2. (a) and (b).

□

Lemma 2. *If $n = p$ is an odd* **prime** *integer then*

$$b_p = 0; \ b_m \equiv (-1)^m (mod\ p) \ for \ 0 \le m \le p-1. \tag{11}$$

Proof. For the first equality see formula (7) above.
For the second congruence we get from formula (7):

$$b_m = (-1)^m \sum_{k=0}^{m} (-1)^k \binom{m}{k} \binom{p}{k}. \tag{12}$$

But $\binom{p}{k} (mod\ p) \equiv 0$ excepting $k = 0$ and $k = p$ when it is $\equiv 1$. Thus here in (12) we need only $k = 0$ and in this first case $b_m \equiv (-1)^m (mod\ p)$ for all $0 \le m \le p-1$. □

Theorem 1. *An odd natural number n is prime iff.*

$$\text{Denominator}\left\langle \binom{n}{n^{-1}} \right\rangle = \text{Denominator} \sum_{m=0}^{n} \binom{n^{-1}}{m} K_m^{(n+m)}(m) = n^{n-1}. \tag{13}$$

Proof. 1. If $n = p$ (prime) then by f. (8) we have $\left\langle \binom{p}{p^{-1}} \right\rangle = \langle A^{(p)} | B^{(p)} \rangle$ and recollecting item (3) of Lemma 1 and formula (10) we get $\left\langle \binom{p}{p^{-1}} \right\rangle = \sum_{m=0}^{p-1} a_m b_m + a_p b_p = \sum_{m=0}^{p-1} \frac{\lambda_m}{p^m} b_m + \frac{\lambda_p}{p^{p+1}} b_p = \frac{Q}{p^{p+1}}$ where $Q - \lambda_p b_p = Q - \lambda_p \cdot 0 = Q = p^2(\lambda_0 p^{p-1} b_0 + \ldots + \lambda_{p-1} b_{p-1})$ hence $\left\langle \binom{p}{p^{-1}} \right\rangle = \frac{Q}{p^{p-1}}$. This fraction is evidently irreducible because $\lambda_{p-1} \cdot b_{p-1} \equiv 1 (mod\ p)$ and so Denominator$\left\langle \binom{p}{p^{-1}} \right\rangle = p^{p-1}$

2. Otherwise, if n is not prime and index s, $1 < s < n$ is such that $\gcd(n, s) > 1$ then n is not inversible modulo s (compare the proof of Lemma 1, item 1) and this s becomes an '*extramultiplier*' (besides n^{n-1}) in the denominator of $\left\langle \binom{n}{n^{-1}} \right\rangle$ and hence this denominator cannot be equal to n^{n-1}.

□

3. Concuding Remark

At the present moment we consider the Neville's algorithm as the most convenient tool for evaluation of the Denominator$\left\langle \binom{n}{n^{-1}} \right\rangle$ *(See theorem 1). The complexity of this algorithm can be estimated as* $\mathrm{O}(n^2)$ [7].

References

[1] Yu. V. Matiyasevich. *'A class of primality criteria formulated in terms of divisibility of binomial coefficicients'*, Zap. Nauchn. Sem. LOMI, 1977, Volume 67, 167–183.

[2] Yu. V. Matiyasevich. *'The Rieman hypothesis as the parity of special binomial coefficients'*, Chebyshevskii sbornik. vol. 19. no 3, 2018. pp. 46–60.

[3] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes.* North-Holland (1977).

[4] N.D. Gogin, Mika Hirvensalo. *'On the moments of squared binomial coefficients'*, 2020, https://pca-pdmi.ru/2020/files/10/GoHi2020ExtAbstract.pdf

[5] S. Beresin and N. P. Jhidkov. *'Computing Methods'*, Pergamon Press, New York 1973.

[6] Nikita Gogin, Mika Hirvensalo. *'Recurrent Construction of MacWilliams and Chebyshev matrices'*, University of Turku, January 2012, https://www.researchgate.net/publication/31597175

[7] Weisstein, Eric W. *'Neville's Algorithm. From MathWorld–A Wolfram Web Resource.'*, https://mathworld.wolfram.com/NevillesAlgorithm.html

Nikita Gogin
e-mail: *ngiri@list.ru*

Vladislav Shubin
e-mail: *v.v.choubine@gmail.com*

Departament of Mathematics
Stockholm State University
Stockholm, Sweden