P-ADIC ORDER OF POSITIVE INTEGERS VIA BINOMIAL COEFFICIENTS

Dario T. de Castro
Instituto Federal do Rio de Janeiro - Campus Nilópolis, Nilópolis, Rio de Janeiro, Brazil
dario.neto@ifrj.edu.br

Received: 1/9/22, Accepted: 6/17/22, Published: 7/8/22

Abstract

We prove a formula for the p-adic order of positive integers that explores divisibility properties of binomial coefficients. A second formula, also in terms of binomial coefficients, is proposed as a conjecture.

1. Introduction

A branch of combinatorics that consistently attracts much attention today is the study of divisibility properties of binomial coefficients. A concept that has been widely used in these studies is the p-adic order of a number [7], represented as $v_p(n)$. For a prime p and a positive integer n, the p-adic order is defined as the exponent of the highest power of p that divides n. It is part of the fundamental theorem of arithmetic which states that every positive integer n has a unique factorization in terms of prime numbers p_i (with $i = 1, 2, 3, ...$), namely,

$$n = \prod_{i=1}^{\infty} p_i^{v_{p_i}(n)}. \tag{1}$$

In this paper, for the p-adic order of positive integers, we present two expressions that explore divisibility properties of binomial coefficients. One of these expressions is proposed as a conjecture. Throughout this study, we shall use the notation $\lfloor x \rfloor$, $\lceil x \rceil$ and $\{x\}$ to indicate, respectively, the largest integer smaller than or equal to x, the smallest integer greater than or equal to x and the fractional part of x. Let us first enunciate two properties of $v_p(n)$ that follow from its definition:

$$v_p(a \cdot b) = v_p(a) + v_p(b) \quad \text{and} \quad v_p(a/b) = v_p(a) - v_p(b), \tag{2}$$

with $a, b \in \mathbb{N}^*$. An expression for the p-adic order of factorials of positive integers obtained by A. M. Legendre [2, 5] is given by

$$v_p(n!) = \sum_{k=1}^{\lfloor \log_p n \rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor . \tag{3}$$

One can also write this formula as

$$v_p(n!) = \frac{n - s_p(n)}{p-1}, \tag{4}$$

where $s_p(n)$ is the sum of the digits of n when represented in base p. That is, when n is written as

$$n = a_0 + a_1 p + a_2 p^2 + ... + a_m p^m, \;\; a_i \in \{0, 1, 2, ..., p-1\}, \tag{5}$$

then

$$s_p(n) = a_0 + a_1 + a_2 + ... + a_m. \tag{6}$$

The p-adic order of binomial coefficients can be evaluated from (4) using the properties in (2). Alternatively, it can be determined by applying E. Kummer's theorem [4], which we enunciate below.

Kummer's Theorem. *The power to which the prime p divides the binomial coefficient $\binom{n}{m}$ is given by the number of 'carries' when we add m and $n-m$ in base p.*

From (2) and (4), a formula for $v_p(n)$ can be derived:

$$\begin{aligned} v_p(n) &= v_p(n!) - v_p((n-1)!) \\ &= \frac{1 - s_p(n) + s_p(n-1)}{(p-1)}. \end{aligned} \tag{7}$$

Other expressions for $v_p(n)$ are possible using functions like $\lfloor x \rfloor$, $\{x\}$ or $\lceil x \rceil$. An example of such formulae is as follows:

$$v_p(n) = \lfloor \log_p n \rfloor - \sum_{j=1}^{\lfloor \log_p n \rfloor} \left\lceil \left\{ \frac{n}{p^j} \right\} \right\rceil . \tag{8}$$

We leave it to the reader to verify this fact.

In the next sections, we shall present two other general expressions for $v_p(n)$ that have a combinatorial appeal, since they are given in terms of binomial coefficients.

2. Auxiliary Results

To derive a formula for $v_p(n)$ grounded on divisibility properties of binomial coefficients, we shall first introduce the function $\beta_k(j,n)$.

Definition 1. With $n, j, k \in \mathbb{N}^*$, let

$$\beta_k(j,n) = k\left\{\binom{n}{k^j}\frac{k^{j-1}}{n}\right\}. \tag{9}$$

This function participates in our first main result, and we shall prove in what follows that it admits a straightforward interpretation as a Boolean operator related to the question of whether k^j divides n when k is a prime number.

Lemma 1. *Given n and j positive integers and p prime, the function $\beta_p(j,n)$ yields 0 if $p^j \nmid n$ and yields 1 if $p^j | n$.*

Proof. Let us consider the two cases separately.

`Case 1:` $p^j \nmid n \Longrightarrow \beta_p(j,n) = 0$

Let Q be a positive integer such that $p^j < Q$ and $p^j \nmid Q$. Taking $\beta_p(j,n)$ as given by (9), we intend to show that, for $n = Q$, the expression

$$\binom{Q}{p^j}\frac{p^{j-1}}{Q} \tag{10}$$

always yields an integer. Since binomial coefficients are known to be integers, we may write

$$\binom{Q}{p^j} = I_0 \in \mathbb{N}^* \tag{11}$$

and

$$\binom{Q-1}{p^j-1} = I_0\frac{p^j}{Q} = I_1 \in \mathbb{N}^*. \tag{12}$$

Additionally, from (10), we have

$$\frac{Q!}{p^j!\,(Q-p^j)!}\,\frac{p^{j-1}}{Q} = \frac{(Q-1)!}{(p^j-1)!\,(Q-p^j)!}\,\frac{p^{j-1}}{p^j} = \frac{I_1}{p}. \tag{13}$$

From (12) and (13), and using the fact that $p^j \nmid Q$, it follows that $p \,|\, I_1$, which implies that expression (10) yields an integer. This concludes the proof for this case.

`Case 2:` $p^j|n \Longrightarrow \beta_p(j,n) = 1$

Let K be a positive integer and let $n = Kp^j$. We intend to prove that $\beta_p(j, Kp^j) = 1$, which means that

$$p\left\{\frac{(Kp^j)!}{p^j!\,((K-1)p^j)!}\,\frac{p^{j-1}}{Kp^j}\right\} = 1. \tag{14}$$

This hypothetical identity can be expressed as

$$\frac{(Kp^j-1)!\,p^{j-1}}{p^j!\,((K-1)p^j)!}=M+\frac{1}{p}, \tag{15}$$

where M is a natural number. Multiplying both sides in (15) by p, the resulting equation can be put equivalently as

$$\binom{Kp^j-1}{p^j-1}\equiv 1 \pmod{p}. \tag{16}$$

Thus, to demonstrate (16), we shall use Lucas' Theorem [6], which we state below.

Lucas' Theorem. *Let p be a prime number and let R and S be positive integers such that*

$$R=r_0+r_1p+r_2p^2+...+r_mp^m\ ,\ \ r_i\in\{0,1,2,...,p-1\}, \tag{17}$$

and

$$S=s_0+s_1p+s_2p^2+...+s_lp^l\ ,\ \ s_i\in\{0,1,2,...,p-1\}, \tag{18}$$

where r_i and s_i are, respectively, the digits of R and S when written in base p. We then have

$$\binom{R}{S}\equiv\prod_{i=0}^{\max\{m,l\}}\binom{r_i}{s_i} \pmod{p}. \tag{19}$$

Here, we adopt the convention $\binom{r}{s}=0$ if s is either greater than r or smaller than zero.

The use of Lucas' congruence relation, with its present notation, to prove (16) requires one to note that:

1. Writing $S=p^j-1$ in base p yields a number of j digits ($l=j-1$), all of them being equal to $p-1$.
2. By representing the number $R=Kp^j-1$ as a sum of two terms, namely p^j-1 and $(K-1)p^j$, we observe that, in base p, R will have in general more than j digits ($m>j-1$ for $K>1$). Additionally, all of its first j digits will also be equal to $p-1$.

From these considerations, we get

$$\binom{R}{S}=\binom{Kp^j-1}{p^j-1}\equiv\left[\binom{p-1}{p-1}^j\times\binom{r_j}{0}\times...\times\binom{r_m}{0}\right] \pmod{p}, \tag{20}$$

which clearly yields $1 \pmod{p}$. □

If q is a composite number, the function $\beta_q(j,n)$ shall not behave as established in Lemma 1 for all $n \in \mathbb{N}^*$. To illustrate this, the next theorem associates an integer $n_{q,j}$ to each pair (q,j), with $j \in \mathbb{N}^*$, so that $\beta_q(j,n_{q,j}) \neq 0$ even though $q^j \nmid n_{q,j}$.

Theorem 1. *Let $q > 0$ be a composite number such that $q = kp^m$, where $m \in \mathbb{N}^*$, p is prime and $p \nmid k$. Given $j \in \mathbb{N}^*$, if $n_{q,j} = q^j + p^{mj-m+1}$, then $\beta_q(j,n_{q,j}) \neq 0$, even though we have $q^j \nmid n_{q,j}$.*

Proof. From (9):

$$\begin{aligned}
\beta_q(j,n_{q,j}) &= q\left\{\binom{q^j + p^{mj-m+1}}{q^j}\frac{q^{j-1}}{q^j + p^{mj-m+1}}\right\} \\
&= q\left\{\binom{q^j + p^{mj-m+1} - 1}{q^j - 1}\frac{1}{q}\right\} \\
&= q\left\{\binom{q^j + p^{mj-m+1} - 1}{p^{mj-m+1}}\frac{1}{q}\right\} \\
&= q\left\{\binom{q^j + p^{mj-m+1} - 1}{p^{mj-m+1} - 1}\frac{q^{j-1}}{p^{mj-m+1}}\right\} \\
&= q\left\{(Mp+1)\,\frac{k^{j-1}}{p}\right\}, \qquad (21)
\end{aligned}$$

where $\binom{q^j+p^{mj-m+1}-1}{p^{mj-m+1}-1} \equiv 1 \pmod p$ from Lucas' Theorem and M is a positive integer. Thus given that $p \nmid k$, we have

$$\beta_q(j,n_{q,j}) = q\left\{\frac{k^{j-1}}{p}\right\} \neq 0. \qquad (22)$$

□

3. Main Results

Since $\beta_p(j,n)$ acts, when p is prime, as a Boolean function related to whether or not p^j divides n, we are now in a position to present our first expression for $v_p(n)$.

Theorem 2. *Let n be a positive integer and p be a prime number. Then, the p-adic order of n can be expressed as*

$$v_p(n) = p\sum_{j=1}^{\lfloor \log_p n\rfloor}\left\{\binom{n}{p^j}\frac{p^{j-1}}{n}\right\}. \qquad (23)$$

Proof. From Lemma 1, it is easy to see that we just have to sum up the terms $\beta_p(j,n)$ for all possibly effective values of j. □

Formula (23) can also be expressed as

$$v_p(n) = \max\left\{ j \in \mathbb{N} : \binom{n-1}{p^j-1} \equiv 1 \pmod{p} \right\}. \tag{24}$$

Remark 1. Let p be a prime number and let n, k and s be integers satisfying $n > 0$, $k > 0$ and $0 \leq s < n$. If $p^k | n$, then the expression

$$\binom{n-1}{s} \equiv (-1)^{s-\lfloor \frac{s}{p} \rfloor} \binom{\frac{n}{p}-1}{\lfloor \frac{s}{p} \rfloor} (\text{mod } p^k), \tag{25}$$

obtained in [1], may be used to recursively demonstrate (24), but only for those values of n such that $v_p(n) \neq 0$.

Remark 2. From Theorems 1 and 2, it follows that the evaluation of $v_q(n)$ using (23) yields correct results for all $n \in \mathbb{N}^*$ if and only if q is prime.

The next corollary follows from Lemma 1.

Corollary 1. *Let n be a positive integer and p be a prime number. Then*

$$\sum_{j=1}^{\lfloor \log_p n \rfloor} \binom{n-1}{p^j-1} \equiv v_p(n) \pmod{p}. \tag{26}$$

Proof. According to Lemma 1, $\binom{n-1}{p^j-1}$ yields one plus a multiple of p if $p^j | n$ and a multiple of p if $p^j \nmid n$. □

Lemma 1 also provides an alternative way to generalize the following proposition (see [3]) that can be obtained from Wilson's theorem, whose statement follows below.

Wilson's Theorem. *An integer $n > 1$ is a prime number if and only if it divides $(n-1)! + 1$.*

Proposition 1. *If m is a positive integer and p is a prime number, then*

$$\binom{mp-1}{p-1} \equiv 1 \pmod{p}. \tag{27}$$

It is clear from our results that a more general congruence relation can be derived, namely

$$\binom{mp^\alpha - 1}{p^\gamma - 1} \equiv 1 \pmod{p}, \tag{28}$$

with $\alpha, \gamma \in \mathbb{N}^*$ and $\alpha \geq \gamma$.

Remark 3. One can alternatively express (23) with the use of complex numbers. The resulting formula reads as follows

$$v_p(n) = \frac{ie^{-i\pi/p}}{2\sin(\pi/p)} \left(\lfloor \log_p n \rfloor - \sum_{j=1}^{\lfloor \log_p n \rfloor} e^{\frac{2\pi i}{p}\binom{n-1}{p^j-1}} \right). \tag{29}$$

We leave the proof of this fact as an exercise to the reader.

We now pose a conjecture on another formula for the p-adic order of positive integers, which is also given in terms of binomial coefficients. Let us first introduce some definitions. In what follows, n is a positive integer, p is a given prime number and p_i is the ith prime number.

Definition 2. Let $\mathcal{S}_{p,n}^{\min}$ and $\mathcal{S}_{p,n}^{\max}$ denote sets of irreducible fractions given by

$$\mathcal{S}_{p,n}^{\min} = \left\{ \frac{1}{n}\binom{n}{p_i^j} \,\middle|\, i \in \mathbb{N}^*,\ j \in \mathbb{N},\ \gcd(p_i, p) = 1,\ p_i^j \leq n \right\}, \tag{30}$$

$$\mathcal{S}_{p,n}^{\max} = \left\{ \frac{1}{n}\binom{n}{k} \,\middle|\, 0 < k \leq n,\ \ \gcd(k, p) = 1 \right\}. \tag{31}$$

Definition 3. A set $\mathcal{S}_{p,n}$ will be called admissible if it satisfies the condition $\mathcal{S}_{p,n}^{\min} \subseteq \mathcal{S}_{p,n} \subseteq \mathcal{S}_{p,n}^{\max}$.

Conjecture 1. Given any admissible set $\mathcal{S}_{p,n}$, the p-adic order of a positive integer n can be expressed as

$$v_p(n) = \log_p \left(\frac{n}{\mathcal{L}_{p,n}} \right), \tag{32}$$

where $\mathcal{L}_{p,n}$ represents the least common denominator of the elements of $\mathcal{S}_{p,n}$.

Remark 4. We observed that elements belonging to $\mathcal{S}_{p,n}$ which are not in $\mathcal{S}_{p,n}^{\min}$ seem to be either redundant or integers.

Remark 5. Conjecture 1 can be regarded as an assertion about $\mathcal{L}_{p,n}$, namely,

$$\mathcal{L}_{p,n} = \frac{n}{p^{v_p(n)}} = \prod_{p_i \neq p} p_i^{v_{p_i}(n)}. \tag{33}$$

Furthermore, computational evidence suggests that the primality of p, as it appears in (32), is a necessary condition if we want this formula to hold for every positive integer n. Thus, to substantiate this statement, we present the following conjecture.

Conjecture 2. Let $q > 0$ be a composite number, p_j a prime number that divides q, and c a non-negative integer. If we take $n = q^c\, p_j$, the evaluation of $v_q(n)$ using (32) will fail for any admissible $\mathcal{S}_{q,n}$.

Remark 6. Together, the two conjectures above suggest that formula (32) for $v_q(n)$ yields correct results for all $n \in \mathbb{N}^*$ if and only if q is prime.

4. Conclusions

We presented two expressions for the p-adic order of a positive integer n. They are given in terms of binomial coefficients that occur in the nth row of Pascal's triangle. From the first expression, we derived a congruence relation which connects $v_p(n)$ with a lacunary sum of the entries in the $(n-1)$th row of Pascal's triangle. The second of these expressions for $v_p(n)$, proposed as a conjecture, was motivated by numerical evidence obtained with the software Wolfram Mathematica. To some extent, we can say that expressions (23) and (32) are complementary. In fact, while $v_p(n)$ is evaluated using powers of p in the former expression, in the latter only powers of primes other than p are used. We believe these expressions also have good pedagogical features, since they (a) represent new connections between p-adic orders and binomial coefficients, (b) may be used in exercises either as identities to be proved or as demonstration tools for other propositions, and (c) contribute to reinforce the distinction between prime and composite numbers. Furthermore, these expressions for $v_p(n)$ being general and of simple structure, seem to indicate the existence of a combinatorial context for the prime number factorization of integers. This possibility, however, remains to be investigated. Finally, we note that the Boolean operator defined in (9) can be used to express other arithmetic functions in terms of binomial coefficients. For instance, the prime omega function $\omega(n)$, which gives the number of prime factors of n, can be represented as $\omega(n) = \sum_{i=1}^{\infty} \beta_{p_i}(1, n)$.

Acknowledgments. The author wishes to thank Professors Cleber Haubrichs, Kevin Ryde and Reinaldo de Melo for helpful and inspiring discussions. Gratitude is also due to the anonymous referee whose comments and suggestions helped improve this manuscript.

References

[1] T. X. Cai, A. Granville, On the residues of binomial coefficients and their products modulo prime powers, *Acta. Math. Sin.*, **18**, No. 2 (2002), 277–288.

[2] L. E. Dickson, *History of the theory of numbers*, Vol. 1, Chelsea Publishing Company, New York, (1952), 263–271.

[3] 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, www.dms.umontreal.ca/∼andrew/Binomial/.

[4] E. Kummer, Über die Ergänzungssätze zu den allgemeinen Reziprozitätsgesetzen, *Journal für die reine und angewandte Mathematik*, **44**, (1852), 93–146.

[5] A. M. Legendre, *Theorie des Nombres*, Firmin Didot Freres, Paris, 1830.

[6] E. Lucas, Theorie des Fonctions Numériques Simplement Périodiques, *Amer. J. Math.*, **1**, (1878), 229–230.

[7] J. W. Sander, A story of binomial coefficients and primes, *Amer. Math. Monthly*, **102**, No. 9 (1995), 802–807.