# Factorials and Integers for Applications in Computing and Cryptography

Chinnaraji Annamalai
School of Management, Indian Institute of Technology, Kharagpur, India
Email: anna@iitkgp.ac.in
https://orcid.org/0000-0002-0992-2584

**Abstract**: Mathematical formulae with integers or prime numbers are used as cryptographic algorithms like RSA algorithm and elliptic-curve cryptography. These methodological advances in computational science and mathematics play a vital role in communication and cybersecurity. This article is prepared for applications in computing and cybersecurity using the theorems in factorials and binomial identity. Also, this paper focuses on the analysis of relationship between factorials and integers.

**MSC Classifications Codes**: 05A10

**Keywords**: algorithm, combinatorics, computation, prime number

## 1. Introduction

Non-negative integers play a crucial role in factorial functions and combinatorial expansions with binomial coefficients [1-9] for building the computational theorems and formulae that are used for algorithms and cryptographic equations. Also, the results of factorials and binomial coefficients are used as strong applications without any vulnerability in computing, management, science, and engineering

### Factorials with Integers

Computational science, binomial distribution, and combinatorics [10-15 are used as powerful applications in computer science and engineering including artificial intelligence, machine learning, communication and cybersecurity. In this article, theorems in factorials with integers are introduced and the relationship between factorials and integers are analyzed for further developments of techniques and formulae in combinatorics.

Thorem 2.1: For any integers $p$ and $q$ such that $q \geq p \geq 0$,

the divisions of factorials , that is , $\frac{q!}{p!}; \frac{(p+q)!}{p!}; \frac{(p+q)!}{q!}$ and $\frac{(p+q)}{p!\,q!}$, are integers.

$Proof.$ $0! = 1;\ 1! = 1;\ 2! = 1 \times 2 = 2;\ 3! = 1 \times 2 \times 3 = 6; \cdots;\ p!$ for $p \geq 0$ are integers. If $q = p \geq 0$, then $q! = p! \geq 1$. If $q > p$, $q! = p! \times (p+1)(p+2)(p+3)\cdots(q-2)(q-1)q$. $\frac{q!}{p!} = (p+1)(p+2)(p+3)\cdots(q-2)(q-1)q$ is an integer. $As$ $\frac{q!}{p!}$ is an integer, $\frac{(p+q)!}{p!}$ $and$ $\frac{(p+q)!}{q!}$ are integers. Let us prove that $\frac{(p+q)!}{p!\,q!}$ $is$ an integer. $\frac{(p+q)!}{p!\,q!} = \frac{(p+1)(p+2)(p+3)\cdots(p+q)}{q!}$. Let $p = 0$. Then, $\frac{(p+1)(p+2)\cdots(p+q)}{q!} = 1$

and let $p = 1. \dfrac{2 \times 3 \times 4 \times \cdots \times q(q+1)}{q!} = \dfrac{q! \times (q+1)}{q!} = q + 1$ is an integer, that is,

$If\ \ p \geq\ 1, \text{then}\ \dfrac{(p+1)(p+2)(p+3)\cdots(p+q)}{q!}\ \geq (q+1)$ are integers for $p = 1, 2, 3, \ldots$

Hence, theorem is proved.

Note that $p! \leq q! \leq p!\, q! \leq (p+q)!\ \Longrightarrow\ \dfrac{(p+q)!}{p!\, q!} \leq \dfrac{(p+q)!}{q!} \leq \dfrac{(p+q)!}{p!}$.

We can also prove the theorem by binomial coefficient.

The binomial coefficient is $\binom{q}{p} = \dfrac{q!}{p!\,(q-p)!}$. If $q = p, \text{then}\ \binom{p}{p} = \dfrac{p!}{p!\,(p-p)!} = 1.$

$If\ q > p, \binom{q}{p} = \dfrac{q!}{p!\,(q-p)!} > 1$ is an integer. $For\ example, \binom{3}{2} = \dfrac{3!}{2!\,1!} = 3.$

Binomial coeffi*cient* $\binom{p+q}{p} = \dfrac{(p+q)!}{p!\, q!} = l$ is an integer, $(l \geq 0)$.

Note that $\dfrac{(p+q)!}{p!\, q!} = l\ \Longrightarrow\ (p+q)! = l \times p! \times q!$.

Theorem 2.2： For any $k$ nonnegative integers $n_1, n_2, n_3, \cdots and\ n_k$,

$(n_1 + n_2 + n_3 + \cdots + n_k)!\ =\ (a_1 \times a_2 \times a_3 \times \cdots \times a_{k-1}) \times n_1! \times n_2! \times n_3! \times \cdots \times n_k!,$

$$\text{that is,} \left(\sum_{i=1}^{k} n_i\right)! = A \prod_{i=1}^{k} n_i\,!,$$

where $A = a_1 \times a_2 \times a_3 \times \cdots \times a_{k-1}$ and $A, a_1, a_2, a_3, \cdots, a_{k-1}$ are nonnegative integers.

Proof.

Let us begin the proof with example: (0+2+1+3)! =A× 0! ×2! ×1! ×3! ⟹720=120×0!×2!×1!×2!
and (0+0+0+1+0+0+0+0)! = A×0!×0!×0!×1!×0!×0!×0!×0! ⟹ 1 = A×1, where A = 1.

Let $x = n_2 + n_3 + n_4 + \cdots + n_k\ .Then, (n_1 + x) = a_1 \times n_1! \times x!$ (refer to theorem 2.1),
that is, $(n_1 + n_2 + n_3 + \cdots + n_k)!\ =\ a_1 \times n_1! \times (n_2 + n_3 + \cdots + n_k)!$.

Similarly, if we apply the same way to prove each of the sums, we get as follows:
$(n_2 + n_3 + n_4 + \cdots + n_k)! = a_2 \times\ n_2! \times (n_3 + n_4 + \cdots + n_k)!;\ \ (n_3 + n_4 + n_5 + \cdots + n_k)! = a_3 \times\ n_3! \times (n_4 + n_5 + \cdots + n_k)!; (n_4 + n_5 + n_6 + \cdots + n_k) = a_4 \times\ n_4! \times (n_5 + n_6 + \cdots + n_k)!;\ , \cdots, and\ (n_{k-1} + n_k) = a_{k-1} \times\ n_{k-1}! \times n_k.$

If we substitute these results step by step in $a_1 \times n_1! \times (n_2 + n_3 + \cdots + n_k)!$, that is,
$a_1 \times n_1! \times (n_2 + n_3 + n_4 \cdots + n_k)! =\ a_1 \times n_1! \times (a_2 \times n_2! \times (n_3 + n_4 \cdots + n_k)!)$
$= a_1 \times a_2 \times n_1! \times n_2! \times (a_3 \times n_3! \times (n_{4+} \cdots + n_k)!)$, etc., we obtain the following result.

$(n_1 + n_2 + n_3 + \cdots + n_k)!\ =\ (a_1 \times a_2 \times a_3 \times \cdots \times a_{k-1}) \times n_1! \times n_2! \times n_3! \times \cdots \times n_k!,$

$$\text{that is,} \left(\sum_{i=1}^{k} n_i\right)! = A \prod_{i=1}^{k} n_i\,!,$$

where $A = a_1 \times a_2 \times a_3 \times \cdots \times a_{k-1}$ and $A, a_1, a_2, a_3, \cdots, a_{k-1}$ are nonnegative integers. Hence, theorem is proved.

For instance, if $n_1 = n_2 = n_3 = \cdots = n_k = n$, then, $(n_1 + n_2 + n_3 + \cdots + n_k)! = (k \times n)!$., where $k, n \geq 0$ are any integer, that is, $k$ & $n$ = 0, 1, 2, 3, 4, 5, . . . .,

If $n_1 = n_2 = n_3 = \cdots = n_k = 0$. Then, $(n_1 + n_2 + n_3 + \cdots + n_k)! = (k \times 0)! = 1$.
If $n_1 = n_2 = n_3 = \cdots = n_k = 1$. Then, $(n_1 + n_2 + n_3 + \cdots + n_k)! = (k \times 1)! = k!$.
If $n_1 = n_2 = n_3 = \cdots = n_k = k$. Then, $(n_1 + n_2 + n_3 + \cdots + n_k)! = (k \times k)! = k^2!$.

This idea can help to the researchers working in computational science, management, science, and engineering.

## 2. Cybersecurity

Computational science is a rapidly growing multi-and inter-disciplinary area where science, engineering, computation, mathematics, and collaboration uses advance computing capabilities to understand and solve the most complex real life problems [12-15]. Cybersecurity is the practice of protecting the computing systems, devices, networks, programs and data from cyber-attacks. Its objective is to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems and networks. For this purposes, we need a strong security mathematical algorithm [10, 11] like RSA algorithm and Elliptic Curve Cryptography. The factorials and binomial coefficients enable computing science to build a strong cryptographic algorithm for the effective information security. The following factorial result can be used as power tool in algorithm and software development.

For any $k$ nonnegative integers $n_1, n_2, n_3, \cdots and\ n_k$,
$(n_1 + n_2 + n_3 + \cdots + n_k)! = (a_1 \times a_2 \times a_3 \times \cdots \times a_{k-1}) \times n_1! \times n_2! \times n_3! \times \cdots \times n_k!$,

$$\text{that is,} \left( \sum_{i=1}^{k} n_i \right)! = A \prod_{i=1}^{k} n_i\,!,$$

where $A = a_1 \times a_2 \times a_3 \times \cdots \times a_{k-1}$ and $A, a_1, a_2, a_3, \cdots, a_{k-1}$ are nonnegative integers.

For example, (0+0+0+1+1+1+0+0+1+1+0)! = A× 0! ×0! ×0! ×1! × 1! ×1! ×0! × 0! ×1! ×1! ×0!, that is, 120=120× 0! ×0! ×0! ×1! × 1! ×1! ×0! × 0! ×1! ×1! ×0! $\Longrightarrow 120 = 120$, where $A = 120$ and 0! ×0! ×0! ×1! × 1! ×1! ×0! × 0! ×1! ×1! ×0! =1. This may be vulnerability for the construction of algorithms. For designing the strong algorithm for application in cybersecurity, the integers or prime numbers of $n_1, n_2, n_3, \cdots, n_k$ must be greater than the integer 1.

## 3. Conclusion

In this article, combinatorial techniques such as factorial and binomial expansions have been introduced for the applications in computational science and cryptography. These methodological advances can enable the researchers working in computational science, management, science and engineering to solve the most real life problems and meet today's challenges [16-20].

## References

**References**


[1] Annamalai C (2022) "Application of Factorial and Binomial identities in Cybersecurity", engr*X*iv. https://doi.org/10.31224/2355.

[2] Annamalai C (2022) "Factorial of Sum of Two nonnegative Integers is equal to Multiple of the Product of Factorial of the Two Nonnegative Integers", OSF Preprints, https://doi.org/10.31219/osf.io/8usry.

[3] Annamalai C (2022) "Application of Factorial and Binomial identities in Computing and Cybersecurity", Research Square. https://doi.org/10.21203/rs.3.rs-1666072/v3.

[4] Annamalai C (2022) Theorems based on Annamalai's Binomial Coefficient and Identity, Zenodo. https://doi.org/10.5281/zenodo.6548228.

[5] Annamalai C (2022) "Application of Factorial and Binomial identities in Cybersecurity and Communications", Research Square. https://doi.org/10.21203/rs.3.rs-1666072/v4.

[6] Annamalai C (2022) "Application of Annamalai's Factorial and Binomial identities in Cybersecurity", OSF Preprints. https://doi.org/10.31219/osf.io/djg34.

[7] Annamalai C (2022) "Application of Factorial and Binomial identities in Communication and Cybersecurity", Research Square. https://doi.org/10.21203/rs.3.rs-1666072/v45.

[8] Annamalai C (2022) "Factorial of Sum of Nonnegative Integers", OSF Preprints. https://doi.org/10.31219/osf.io/cb72k.

[9] Annamalai C (2022) "Factorial of Sum of Nonnegative Integers for Computing and Algorithms", Zenodo. https://doi.org/10.5281/zenodo.6612724.

[10] Annamalai C (2022) "Ascending and Descending Orders of Annamalai's Binomial Coefficient", SSRN Electronic Journal. http://dx.doi.org/10.2139/ssrn.4109710.

[11] Annamalai C (2022) "Combinatorial Relation of Optimized Combination with Permutation", SSRN Electronic Journal. https://dx.doi.org/10.2139/ssrn.4057425.

[12] Annamalai C (2022) "Theorems based on Annamalai's Binomial Coefficient and Identity", SSRN Electronic Journal. http://dx.doi.org/10.2139/ssrn.4109904.

[13] Annamalai C (2022) "Differentiation and Integration of Annamalai's Binomial Expansion", SSRN Electronic Journal. http://dx.doi.org/10.2139/ssrn.4110255.

[14] Annamalai C (2022) "Analysis of the Relationship between Integers and Factorial Functions", OSF Preprints. https://doi.org/10.31219/osf.io/r27s6.

[15] Annamalai C (2022) "Application of Factorial and Binomial Identities in Communications, Information and Cybersecurity", Research Square.

https://doi.org/10.21203/rs.3.rs-1666072/v6.

[16] Annamalai C (2022) "Intuitionistic Fuzzy Sets and Combinatorial Techniques in Computation and Weather Analysis", engr*X*iv. https://doi.org/10.31224/2387.

[17] Annamalai C (2010) "Application of Exponential Decay and Geometric Series in Effective Medicine", Advances in Bioscience and Biotechnology, Vol. 1(1), pp 51-54. https://doi.org/10.4236/abb.2010.11008.

[18] Annamalai C (2012) "Modelling exponential decay to predict half-life of radioactive substance", Journal of Scientific and Mathematical Research, Vol. 6, pp 1-3. https://doi.org/10.5281/zenodo.6614430.

[19] Annamalai C (2014) "Intuitionistic Fuzzy Sets: New Approach and Applications", International Journal of Research in Computer and Communication Technology, Vol. 3(3), pp 283-285. http://ssrn.com/abstract=4100670.

[20] Annamalai C (2019) "Algorithmic Computation of Annamalai's Geometric Series and Summability", Mathematics and Computer Science, Vol. 3(5), pp 100-101. https://doi.org/10.11648/j.mcs.20180305.11.