Some remarks on Kurepa’s left factorial

Bernd C. Kellner

Abstract

We establish a connection between the subfactorial function $S(n)$ and the left factorial function of Kurepa $K(n)$. Some elementary properties and congruences of both functions are described. Finally, we give a calculated distribution of primes below 10000 of $K(n)$.

Keywords: Left factorial function, subfactorial function, derangements

Mathematics Subject Classification 2000: 11B65

1 Introduction

The subfactorial function is defined by

$$S(n) = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}, \quad n \in \mathbb{N}_0$$

which gives the number of permutations of $n$ elements without any fixpoints, also called derangements of $n$ elements, see [6, p. 195]. This was already proven by P. R. de Montmort [2] in 1713. L. Euler [3] independently gave a proof in 1753, see also [4]. This function has the properties ($e \approx 2.71828$ is Euler’s number)

$$S(n) = n S(n-1) + (-1)^n, \quad (1.1)$$
$$S(n) = (n-1) (S(n-1) + S(n-2)), \quad (1.2)$$
$$S(n) = \left\lfloor \frac{n!}{e} \right\rfloor + \delta_n \quad \text{with} \quad \delta_n = \begin{cases} 0, & 2 \nmid n \\ 1, & 2 \mid n \end{cases} \quad (1.3)$$

Kurepa’s left factorial function is defined by

$$K(0) = 0, \quad K(n) = \sum_{k=0}^{n-1} k!, \quad n \in \mathbb{N}.$$  

In 1971 D. Kurepa [8] introduced the left factorial function which is denoted by $!n = K(n)$. Sometimes the subfactorial function is also denoted by $!n$, so we do not use this notation to avoid confusion. For more details of the following conjecture see a overview of A. Ivić and Ž. Mijajlović [7].
Conjecture 1.1 (Kurepa’s left factorial hypothesis)
The following equivalent statements hold

\[
(K(n), n!) = 2, \quad n \geq 2, \\
K(n) \not\equiv 0 \pmod{n}, \quad n > 2, \\
K(p) \not\equiv 0 \pmod{p}, \quad p \text{ odd prime}. 
\]

Recently, D. Barsky and B. Benzaghou [1] have given a proof of this hypothesis. Since \(K(n)\) is also related to Bell numbers \(B_n\) via

\[
K(p) \equiv B_{p-1} - 1 \pmod{p}
\]

for any prime \(p\), they actually proved that \(B_{p-1} \not\equiv 1 \pmod{p}\) is always valid for any odd prime \(p\).

Gessel [5, Sect. 7/10] gives some recursive identities of \(S(n)\), \(B_n\), and others with umbral calculus. Define symbolically \(S^n = S(n)\) and \(B^n = B_n\) with \(S^0 = B^0 = 1\), then one may write

\[
B^{n+1} = (B + 1)^n \quad \text{and} \quad n! = (S + 1)^n, \quad n \geq 0. \tag{1.4}
\]

Interestingly, both sequences have the same property as follows.

Lemma 1.2 Let \(p\) be a prime. Then

\[
\sum_{k=0}^{p} (-1)^k B_k \equiv \sum_{k=0}^{p} (-1)^k S(k) \equiv 0 \pmod{p}
\]

with

\[
B_p \equiv 2 \pmod{p} \quad \text{and} \quad S(p) \equiv -1 \pmod{p}.
\]

Proof. By (1.1) and Wilson’s theorem, we have \(S(p) \equiv -1 \equiv (p - 1)! \pmod{p}\). Hence, we can rewrite (1.4) by \(B^p \equiv (B + 1)^{p-1}\) and \(S^p \equiv (S + 1)^{p-1} \pmod{p}\). Since \(\binom{p-1}{k} \equiv (-1)^k \pmod{p}\) for \(0 \leq k < p\), this provides the proposed congruence. Now, we use a congruence of Touchard for Bell numbers, see [5, Sect. 10, Theorem 10.1]. Then

\[
B_{n+p} - B_{n+1} - B_n \equiv 0 \pmod{p}, \quad n \geq 0.
\]

With \(n = 0\) and \(B_0 = B_1 = 1\), we obtain \(B_p \equiv 2 \pmod{p}\). \(\square\)

First values of \(K(n)\), \(S(n)\), and \(B_n\) are given in the following table.

| \(n\) | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| \(K(n)\) | 0 | 1 | 2 | 4 | 10 | 34 | 154 | 874 | 5914 | 46234 | 409114 |
| \(S(n)\) | 1 | 0 | 1 | 2 | 9 | 44 | 265 | 1854 | 14833 | 133496 | 1334961 |
| \(B_n\) | 1 | 1 | 2 | 5 | 15 | 52 | 203 | 877 | 4140 | 21147 | 115975 |
2 Congruences between $K(n)$ and $S(n)$

Lemma 2.1 Let $n$ be a positive integer, then

$$K(n) \equiv (-1)^{n-1} S(n-1) \pmod{n}.$$ 

Proof. Case $n = 1$ is trivial. Let $n \geq 2$. Then we have

$$(−1)^{n−1}S(n−1) = \sum_{k=0}^{n-1} (-1)^{n−1−k} \left(\begin{array}{c} n−1 \\ k \end{array}\right) (n−1−k)! = \sum_{k=0}^{n-1} (-1)^{k} \left(\begin{array}{c} n−1 \\ k \end{array}\right) k!$$

by turning the summation. Since it is valid for $0 \leq k < n$

$$(−1)^{k} \left(\begin{array}{c} n−1 \\ k \end{array}\right) k! = (-1)^{k} (n−1)\cdots(n−k) \equiv k! \pmod{n},$$

this provides, term by term, the congruence claimed above. □

By Lemma 2.1 and (1.3), we easily obtain a generalization, however, which is only noted for primes elsewhere.

Corollary 2.2 Let $n$ be a positive integer, then

$$K(n) \equiv (-1)^{n-1} \left\lfloor \frac{(n−1)!}{e} \right\rfloor + \delta_{n-1} \pmod{n}.$$ 

Hence, (KH) is equivalent to

$$\left\lfloor \frac{(n−1)!}{e} \right\rfloor \not\equiv -\delta_{n-1} \pmod{n}, \quad n > 2,$$

while by recursive property (1.1)

$$\left\lfloor \frac{n!}{e} \right\rfloor \equiv -\delta_{n-1} \pmod{n}, \quad n \geq 1$$

is always valid.

Corollary 2.3 Let $n$ be a positive integer, then (KH) is equivalent to

$$\left\lfloor \frac{n!}{e} \right\rfloor - \left\lfloor \frac{(n−1)!}{e} \right\rfloor \equiv 0 \pmod{n} \iff n = 1, 2.$$ 

Lemma 2.4 Let $p$ be a prime, then

$$K(p) - K(p - l) \equiv -\frac{S(l-1)}{(l-1)!} \pmod{p}, \quad l = 1, \ldots, p.$$ 

3
Proof. Let \( l \in \{1, \ldots, p\} \). We then have
\[
K(p) - K(p - l) = \sum_{k=p-l}^{p-1} k! = \sum_{k=1}^{l} (p - k)! \equiv \sum_{k=1}^{l} \frac{(-1)^k}{(k-1)!} = -S(l - 1) \cdot \frac{l}{(l-1)!} \quad \text{(mod } p),
\]
since
\[
(p - k)! \equiv \frac{(-1)^k}{(k-1)!} \quad \text{(mod } p) \tag{2.1}
\]
follows by Wilson’s theorem. \( \square \)

**Corollary 2.5** Let \( p \) be an odd prime, then \((KH)\) implies for \( 0 \leq l < p \)
\[
K(p - 1 - l) \not\equiv \frac{S(l)}{l!} \quad \text{(mod } p)
\]
respectively
\[
l! K(p - 1 - l) \not\equiv \left\lfloor \frac{l!}{e} \right\rfloor + \delta_l \quad \text{(mod } p).
\]
Since \((KH)\) is true, we obtain, as an example, the following congruences
\[
K(p) \not\equiv 0, \ K(p - 1) \not\equiv 1, \ K(p - 2) \not\equiv 0, \ K(p - 3) \not\equiv \frac{1}{2}, \ K(p - 4) \not\equiv \frac{1}{3} \quad \text{(mod } p).
\]

3 Properties of \( K(n) \)

To describe some interesting properties of \( K(n) \), we introduce the following definition which we name after Kurepa.

**Definition 3.1** Let \( p \) be an odd prime. The pair \((p, n)\) is called a Kurepa pair if \( p^r \mid K(n) \) with some integer \( r \geq 1 \). The max. integer \( r \) is called the order of \((p, n)\). The index of \( p \) is defined by
\[
i_K(p) = \#\{n : (p, n) \text{ is a Kurepa pair}\}.
\]
If \( i_K(p) > 0 \), then \( p \) is called a Kurepa prime.

We have, e.g., the Kurepa pairs \((19, 7)\), \((19, 12)\), and \((19, 16)\). If \((KH)\) would fail at an odd prime \( p \), then this would imply \( i_K(p) = \infty \). This is an easy consequence of
\[
p \mid K(p), \ p \mid (p + m)! \quad \text{for } m \geq 0.
\]
The case \( p = 2 \) is handled separately. One easily sees that \( 2 \mid K(n) \) for \( n \geq 2 \) and \( K(n) \equiv 2 \pmod{4} \) for \( n \geq 4 \). First values of \( i_K(p) \) are given in the following table.

| \( p \) | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 | 41 | 43 | 47 | 53 | 59 | 61 |
|-------|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| \( i_K(p) \) | 0 | 1 | 1 | 1 | 0 | 1 | 3 | 1 | 0 | 2 | 1 | 2 | 0 | 0 | 0 | 0 | 1 |
Theorem 3.2 Let \((p, n)\) be a Kurepa pair. Then \(p > n > 3\) is valid with
\[ K(p) \equiv (-1)^n n! S(p - 1 - n) \pmod{p} \]
which implies \(p \nmid S(p - 1 - n)\). Furthermore one has \(i_K(p) \leq \left\lfloor \frac{p - 1}{4} \right\rfloor\). Consequently, there exist infinitely many Kurepa primes.

Proof. For now, let \(p\) be an odd prime. Let \((p, n)\) be a Kurepa pair. Since \(p \nmid K(p + m)\) for \(m \geq 0\) by validity of \((K)\) and first values of \(K(\cdot)\) are 0, 1, 2, 4, this yields \(p > n > 3\).

We use Lemma 2.4 with \(n = p - l\), then we have
\[ 0 \not\equiv K(p) - K(n) \equiv \frac{S(p - 1 - n)}{(p - 1 - n)!} \pmod{p} \]
which provides the result by means of (2.1) and also \(p \nmid S(p - 1 - n)\). Now, we have to count possible Kurepa pairs. Corollary 2.5 shows that \(K(p - 2) \not\equiv 0 \pmod{p}\). If \(p \mid K(n)\) then \(p \nmid K(n + l)\) for \(l = 1, 2, 3\). This is seen by \(n! \not\equiv 0 \pmod{p}\) and
\[ n! + (n + 1)! = (n + 2)! \not\equiv 0, n! + (n + 1)! + (n + 2)! = (n + 2)^2 n! \not\equiv 0 \pmod{p}, \]
since \(n \neq p - 2\). On the other side, we have \(4 \leq n \leq p - 1\). Then a simple counting argument provides \(i_K(p) \leq \left\lfloor \frac{p - 1}{4} \right\rfloor\). Finally, \(K(n) \to \infty\) for \(n \to \infty\) and \(p \mid K(n)\) \Rightarrow \(p > n\) for odd primes imply infinitely many Kurepa primes. □

Now, the remarkable fact of \(K(n)\) is the finiteness of Kurepa pairs for all odd primes.

In \(p\)-adic analysis, the series
\[ K(\infty) = \sum_{k=0}^{\infty} k! \]
is an example of a convergent series resp. \(K(n)\) is a convergent sequence which lies in \(\mathbb{Z}_p\), the ring of \(p\)-adic integers. Then \((K)\) is equivalent to \(K(\infty)\) is a unit in \(\mathbb{Z}_p\) for all odd primes \(p\). The behavior \((\pmod{p^r})\) is illustrated by the following theorem. Note that \(l_r\) is related to the so-called Smarandache function for factorials.

Theorem 3.3 Let \(p, r\) be positive integers with \(p\) prime. Then the sequence
\[ K(n) \pmod{p^r}, \quad n \geq 0 \]
is constant for \(n \geq l_r p\) with \(r \geq l_r\) and
\[ l_r = \min_l \left\{ l : l + \frac{l - \sigma_p(l)}{p - 1} \geq r \right\}, \]
where \(\sigma_p(l)\) gives the sum of digits of \(l\) in base \(p\).

Proof. We have to determine a minimal \(l\) with the property \(\text{ord}_p(lp)! \geq r\). Counting factors which are divisible by \(p\), we obtain
\[ \text{ord}_p(lp)! = l + \text{ord}_p l! = l + \frac{l - \sigma_p(l)}{p - 1} \]
by means of the \(p\)-adic valuation of factorials, see [9, Section 3.1, p. 241]. □
At the end, we give some results of calculated Kurepa pairs. There are $N = \pi(10000) - 1 = 1228$ odd primes below 10000. Let $N_r$ be the number of odd primes with index $i_K(p) = r$ in this range. The following table shows the distribution of the index $i_K$.

| $r$ | 0   | 1   | 2   | 3   | 4   | 5   |
|-----|-----|-----|-----|-----|-----|-----|
| $N_r$ | 459 | 472 | 213 | 58  | 23  | 3   |
| $N_r/N$ | 0.37378 | 0.38436 | 0.17345 | 0.04723 | 0.01873 | 0.00244 |

The calculated Kurepa pairs with index $i_K(p) = 5$ are as follows.

|     |     |     |     |     |     |
|-----|-----|-----|-----|-----|
| (2203,277) | (2203,788) | (2203,837) | (2203,1246) | (2203,1927) |
| (5227,850) | (5227,1752) | (5227,3451) | (5227,4363) | (5227,4716) |
| (6689,1716) | (6689,2404) | (6689,3641) | (6689,3969) | (6689,6601) |

All primes below 10000 appear with a simple power in $K(n)$, except $K(3) = 4$. On the other side, the occurrence of higher powers $p^r$ in $K(n)$ seems to be very rare. M. Zivkovic [10] gives the first example $54503^2 \mid K(26541)$. There are two Kurepa pairs $(54503,26541)$ and $(54503,49783)$, but only the first of them has order two.

One may ask whether the distribution of Kurepa pairs resp. the index $i_K$ can be asymptotically determined and even proven. Are there infinitely many non-Kurepa primes $p$ with $i_K(p) = 0$? It seems that this subject of $K(n)$ and its distribution of primes will be much simpler to attack as, for example, the more complicated but in a sense similar case of the distribution of irregular primes of Bernoulli numbers.

**Acknowledgement**

The author wishes to thank Prof. Ivić for informing about the problem of Kurepa.

Bernd C. Kellner  
address: Reitstallstr. 7, 37073 Göttingen, Germany  
email: bk@bernoulli.org

**References**

[1] D. Barsky and B. Benzaghoul. Nombres de Bell et somme de factorielles. *Journal de Théorie des Nombres de Bordeaux*, 16:1–17, 2004.

[2] P. R. de Montmort. Essai d’analyse sur les jeux de hasard. *2nd Edition of 1713, Paris, (reprinted in Annotated Readings in the History of Statistics, Springer-Verlag, 2001, 25–29)*, 130–143, 1713.

[3] L. Euler. Calcul de la probabilité dans le jeu de rencontre. *Memoires de l’académie des sciences de Berlin*, 7:255–270, 1753.

[4] L. Euler. Solutio quaestionis curiosae ex doctrina combinationum. *Memoires de l’académie des sciences de St.-Petersbourg*, 3:57–64, 1811.
[5] I. M. Gessel. Applications of the classical umbral calculus. *Algebra Universalis*, 49:397–434, 2003. arXiv:math.CO/0108121

[6] R. L. Graham, D. E. Knuth, and O. Patashnik. *Concrete Mathematics*. Addison-Wesley, Reading, MA, USA, 1994.

[7] A. Ivić and Ž. Mijajlović. On Kurepa’s Problems in Number Theory. *Publ. Inst. Math.*, 57(71):19–28, 1995. arXiv:math.NT/0312202

[8] D. Kurepa. On the left factorial function !n. *Math. Balkan.*, 1:147–153, 1971.

[9] A. M. Robert. *A Course in p-adic Analysis*, volume 198 of *Graduate Texts in Mathematics*. Springer-Verlag, 2000.

[10] M. Zivkovic. The number of primes \(\sum_{i=1}^{n} (-1)^{n-i} i!\) is finite. *Math. Comp.*, 68:403–409, 1999.