Filomat 29:10 (2015), 2207–2215
DOI 10.2298/FIL1510207M

Published by Faculty of Sciences and Mathematics,
University of Niš, Serbia
Available at: http://www.pmf.ni.ac.rs/filomat

The Kurepa-Vandermonde matrices arising from Kurepa's left factorial hypothesis

Romeo Meštrović[a]

[a]*Maritime Faculty, University of Montenegro, Dobrota 36, 85330 Kotor, Montenegro*

Abstract. Kurepa's (left factorial) hypothesis asserts that for each integer $n \geq 2$ the greatest common divisor of $!n := \sum_{k=0}^{n-1} k!$ and $n!$ is 2. It is known that Kurepa's hypothesis is equivalent to

$$\sum_{k=0}^{p-1} \frac{(-1)^k}{k!} \not\equiv 0 \pmod{p} \quad \text{for each odd prime} \quad p,$$

or equivalently, $S_{p-1} \not\equiv 0 (\mathrm{mod}\, p)$ (i.e., $B_{p-1} \not\equiv 1 (\mathrm{mod}\, p)$) for each odd prime p, where S_{p-1} and B_{p-1} are the $(p-1)$th derangement number and the $(p-1)$th Bell number, respectively. Motivated by these two reformulations of Kurepa's hypothesis and a congruence involving the Bell numbers and the derangement numbers established by Z.-W. Sun and D. Zagier [28, Theorem 1.1], here we give two "matrix" formulations of Kurepa's hypothesis over the field $\mathbb{F}_p$, where p is any odd prime. The matrices V_p and C_p which are involved in these "matrix" formulations of Kurepa's hypothesis are the square $(p-1)\times(p-1)$ Vandermonde-like matrices. Accordingly, V_p and C_p are called the Kurepa-Vandermonde matrices. Furthermore, for each odd prime p we determine $\det(V_p)$ and $\det(C_p)$ in the field $\mathbb{F}_p$.

1. Remarks on Kurepa's hypothesis

In 1971 Dj. Kurepa [12] introduced the *left factorial function* $!n$ which is defined as

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

$!n$ is the Sloane's sequence A003422 in [25].

For more details of the following conjecture proposed by Kurepa in [12] and its reformulations see a overview of A. Ivić and Ž. Mijajlović [8].

Conjecture 1.1 (Kurepa's left factorial hypothesis). *For each positive integer $n \geq 2$ the greatest common divisor of $!n$ and $n!$ is 2.*

2010 *Mathematics Subject Classification*. Primary 05A10; Secondary 11B65, 11B73, 11A05, 11A07
Keywords. Left factorial function, Kurepa's hypothesis, derangement number, reformulation of Kurepa's hypothesis, Bell number, Kurepa's determinant, congruence modulo a prime, Kurepa-Vandermonde matrix, Kurepa-Vandermonde determinant
Received: 01 September 2014; Accepted: 27 February 2015
Communicated by Miroslav Ćirić
Email address: romeo@ac.me (Romeo Meštrović)

Kurepa's hypothesis and its equivalent formulation appear in R. Guy's classic book [7] as problem B44 which asserts that

$$!n \not\equiv 0 \pmod{n} \quad \text{for all } n > 2.$$

Alternating sums of factorials $\sum_{k=1}^{n-1}(-1)^{k-1}k!$ are involved in Problem B43 in [7] which was solved by M. Živković [32].

Further, Kurepa's hypothesis was tested by computers for $n < 1000000$ by Mijajlović and Gogić in 1991 (see, e.g., [17] and [11]).

Kurepa's left factorial hypothesis (or in the sequel, written briefly *Kurepa's hypothesis*) is an unsolved problem since 1971 and there seems to be no significant progress in solving it. Notice that a published proof of Kurepa's hypothesis in 2004 by D. Barsky and B. Benzaghou [1, Théorème 3, p. 13] contains some irreparable calculation errors in the proof of Theorem 3 of this article, and this proof is therefore withdrawn [2].

However, there are several statements equivalent to Kurepa's hypothesis (see, e.g., Kellner [10, Conjecture 1.1 and Corollary 2.3], Ivić and Mijajlović [8], Mijajlović [16, Theorem 2.1], Petojević [21] and [22, Subsection 3.3], Petojević, Žižović and Cvejić [23, Theorems 1 and 2], Šami [30], Stanković [26] and Živković [32]). Moreover, there are numerous identities involving the left factorial function $!n$ and related generalizations (see Carlitz [3], Milovanović [18], Petojević and Milovanović [19], Slavić [24], Stanković [26], Stanković and Žižović [27]). Kurepa's hypothesis is closely related to the Sloane's sequences A049782, A051396, A051397, A052169, A052201, A054516 and A056158 [25].

It was proved by Dj. Kurepa [12, p. 149, Theorem 2.4] that Kurepa's hypothesis is equivalent to the assertion that $!p \not\equiv 0 \pmod{p}$ for all odd primes p. This reformulation was modified by Ž. Mijajlović [12, p. 149, Theorem 2.4] who proved that Kurepa's hypothesis is equivalent to the assertion that

$$\sum_{k=0}^{p-1} \frac{(-1)^k}{k!} \not\equiv 0 \pmod{p} \quad \text{for each prime} \quad p \geq 3. \tag{1}$$

Usually, here as always in the sequel, for rational numbers a/b and c/d such that the integers b and d are not divisible by a prime p, the congruence $a/b \equiv c/d \pmod{p}$ means that $ad - bc \equiv 0 \pmod{p}$.

Notice that

$$S_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}, \quad n = 0, 1, 2, \ldots \tag{3}$$

is the *subfactorial function* whose values are the well known *derangement numbers* which give the number of permutations of n elements without any fixpoints (Sloane's sequence A000166 in [25] whose terms $S_0, S_1, \ldots, S_8$ are as follows: $1, 0, 1, 2, 9, 44, 265, 1854, 14833$). In `Mathematica` 8 the code `Subfactorial[n]` gives the derangement number S_n.

Furthermore, by Wilson theorem, for any prime p we have,

$$S_{p-1} \equiv -\sum_{k=0}^{p-1} \frac{(-1)^k}{k!} \pmod{p}. \tag{4}$$

Remark 1.2. *In* 1999 *M. Živković [32, Table 1] verified that* $S_{p-1} := \sum_{k=0}^{p-1}(-1)^k/k! \not\equiv 0 \pmod{p}$ *for all odd primes* p *less than* $2^{23} = 8388608$. *Searching for the* $r_p := S_{p-1} \pmod{p}$ *for all primes* p *less than* $2^{26} = 67108864$ *and less than* $2^{27} = 134217728$, *was continued in* 2000 *by Y. Gallot [5], and in* 2004 *by P. Jobling [9], respectively. M. Tatarević [31] continued the search of the* r_p *up to* $p < 10^9$. *By all these computational searches, no solution to* $S_{p-1} \equiv 0 \pmod{p}$ *was discovered.*

Notice also that under the validity of heuristic arguments presented in [14, Remarks 1*], based on a classical asymptotic formula of Mertens* (*see, e.g., [4, p. 94]*) *and "log log philosophy"* (*see, e.g., [13]*), *it can be expected one prime less than* 10^{19} *which is "a counterexample" to Kurepa's hypothesis* (*i.e., one prime* $p < 10^{19}$ *for which* $S_{p-1} \equiv 0 \pmod{p}$).

A motivation for the notion of Kurepa's determinant (see [14]) comes from the above equivalent form of Kurepa's hypothesis due to Mijajlović [16]. Using a Linear Algebra approach to the system of $p-2$ homogeneous linear congruences modulo a prime $p \geq 5$ involving the derangement numbers $S_1, S_2, \ldots, S_{p-2}$, in [14] and [15] the author of this article defined the so-called Kurepa's determinant K_n for every integer $n \geq 7$. Namely, by [14, Section 2, Definition 1] for any integer $n \geq 7$ the *Kurepa's determinant* K_n of order $n-4$ is defined as

$$K_n := \begin{vmatrix} 1 & 1 & 1 & 1 & 1 & 1 & \ldots & 1 & 1 & 1 & 1 & 3 \\ 3 & 1 & 1 & 1 & 1 & 1 & \ldots & 1 & 1 & 1 & 1 & 2 \\ 1 & 4 & 1 & 1 & 1 & 1 & \ldots & 1 & 1 & 1 & 1 & 2 \\ 0 & 1 & 5 & 1 & 1 & 1 & \ldots & 1 & 1 & 1 & 1 & 2 \\ 0 & 0 & 1 & 6 & 1 & 1 & \ldots & 1 & 1 & 1 & 1 & 2 \\ 0 & 0 & 0 & 1 & 7 & 1 & \ldots & 1 & 1 & 1 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 & 8 & \ldots & 1 & 1 & 1 & 1 & 2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & \ldots & 0 & 1 & n-4 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 1 & -4 \end{vmatrix}. \tag{5}$$

The Kurepa's determinant K_n with $n \geq 7$ is given by N.J.A. Sloane as the OEIS sequence A236401 [25], where its computation is implemented in `Maple`. For computations of the Kurepa's determinants K_{2n+5} (of odd order $2n+1$) it is used in [14] a code in `Mathematica` 8.

Remark 1.3. *It is proved in [15]* (*also see [14, Theorem 1]*) *that Kurepa's hypothesis is equivalent with the assertion that* $K_p \not\equiv 0 \pmod{p}$ *for all primes* $p \geq 7$.

In the first version of the paper [14] it is proposed the following conjecture [14, Conjecture 2] which in view of Remark 1.3 implies Kurepa's hypothesis, and thus it may be considered as the *strong Kurepa's hypothesis*.

Conjecture 1.4 (The strong Kurepa's hypothesis). *For each integer* $n \geq 7$ *the Kurepa's determinant* K_n *is not divisible by* n.

It is proved in [14, Theorem 2] that the strong Kurepa's hypothesis holds for each even integer $n \geq 8$. On the other hand, it is showed in [14, Theorem 3] that for $n = 11563 = 31 \times 373$ we have $K_{11563} \equiv 0 \pmod{11563}$, and hence, "the odd composite part" of strong Kurepa's hypothesis is not true. The "prime" part of strong Kurepa's hypothesis asserts that $K_p \not\equiv 0 \pmod{p}$ for each prime $p > 5$. This part is by [14, Proposition 1 and Theorem 1] (which is proved in [15]) equivalent to Kurepa's hypothesis.

2. The main results

The derangement numbers S_n defined by (3) are closely related to the *Bell numbers* B_n given by the recurrence

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k, \quad n = 0, 1, 2, \ldots,$$

with $B_0 = 1$ (see, e.g., [6, p. 373]). B_n gives the number of partitions of a set of cardinality n. This is Sloane's sequence A000110 in [25] whose terms $B_0, B_1, \ldots, B_8$ are as follows: $1, 1, 2, 5, 15, 52, 203, 877, 4140$. In `Mathematica` 8 the code `BellB[n]` gives the Bell number.

It is known (see, e.g., [28, Corollary 1.3]) that for any prime p we have

$$B_{p-1} - 1 \equiv S_{p-1} \pmod{p}. \tag{6}$$

Summarizing the reformulations of Kurepa's hypothesis given in Remark 1.3 and by (1), and in in view of the congruences (4) and (6), we immediately get the following result.

Proposition 2.1. *The following statements are equivalent:*

(i) Kurepa's hypothesis holds;

(ii) $B_{p-1} \not\equiv 1 (\mathrm{mod}\ p)$ *for each odd prime* p*;*

(iii) $S_{p-1} \not\equiv 0 (\mathrm{mod}\ p)$ *for each odd prime* p*;*

(iv) $K_p \not\equiv 0 (\mathrm{mod}\ p)$ *for each prime* $p \geq 7$*.*

The idea of the proof of Kurepa's hypothesis given by D. Barsky and B. Benzaghou in 2004 [1, Théorème 3, p. 13] (for a related discussion see [29, Section 4]) is to consider what is known as the Artin-Schreier extension $\mathbb{F}_p[\theta]$ of the field $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ of p elements, where θ is a root (in the algebraic closure of $\mathbb{F}_p$) of the polynomial $x^p - x - 1$. This is a cyclic Galois extension of degree p over $\mathbb{F}_p$. Note that the other roots of $x^p - x - 1$ are $\theta + i$ for $i = 1, 2, \ldots, p-1$. The reason this field extension comes up naturally as follows. The generating series $F(x)$ of the Bell numbers can be evaluated modulo p; this means one computes a "simpler" series $F_p(x)$ such that $F(x) - F_p(x)$ has all coefficients multiples of p, where

$$F(x) = \sum_{n=0}^{\infty} B_n x^n = \sum_{n=0}^{\infty} \frac{x^n}{(1-x)(1-2x)\cdots(1-nx)}$$

is the generating function for B_n's. Since Kurepa's hypothesis is about the Bell numbers B_{p-1} considered modulo p, it makes sense to consider $F_p(x)$ rather than $F(x)$. By using this idea, D. Barsky and B. Benzaghou [1, Théorème 3, p. 13] proved that $B_{p-1} \not\equiv 1 (\mathrm{mod}\ p)$ for any prime p. However, as noticed above, **this proof contains some irreparable calculation errors** [2].

Definition 2.2. *Let* p *be a prime, and let* $A = (a_{ij})_{1 \leq i \leq m}^{1 \leq j \leq n}$ *and* $B = (b_{ij})_{1 \leq i \leq m}^{1 \leq j \leq n}$ *be the* $m \times n$ *matrices whose all entries* a_{ij} *and* b_{ij} $(i = 1, \ldots, m;\ j = 1, \ldots, n)$ *are integers. As usually, we say that the matrices* A *and* B *are equal in the field* $\mathbb{F}_p$ *if* $a_{ij} \equiv b_{ij} (\mathrm{mod}\ p)$ *for all* $i = 1, \ldots, m;\ j = 1, \ldots, n$*, and in this case we write* $A =^p B$*.*

Accordingly to Proposition 2.1, an odd prime p is said to be a counterexample to Kurepa's hypothesis if and only if $S_{p-1} \equiv 0 (\mathrm{mod}\ p)$ (or equivalently, $B_{p-1} \equiv 1 (\mathrm{mod}\ p)$). Motivated by the congruence involving the Bell numbers and the derangement numbers established in 2011 by Z.-W. Sun and D. Zagier [28, Theorem 1.1] (the congruence (14) of Lemma 3.1 in the next section), here we prove the following result.

Theorem 2.3. *An odd prime* p *is a counterexample to Kurepa's hypothesis if and only if in the field* $\mathbb{F}_p$ *there holds*

$$\begin{pmatrix} 1 & (p-1)^{p-2} & (p-1)^{p-3} & \ldots & (p-1) \\ 1 & (p-2)^{p-2} & (p-2)^{p-3} & \ldots & (p-2) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 2^{p-2} & 2^{p-3} & \ddots & 2 \\ 1 & 1 & 1 & \ldots & 1 \end{pmatrix} \begin{pmatrix} B_0 \\ B_1 \\ B_2 \\ \vdots \\ B_{p-2} \end{pmatrix} =^p \begin{pmatrix} S_0 \\ -S_1 \\ S_2 \\ \vdots \\ -S_{p-2} \end{pmatrix}, \tag{7}$$

or equivalently,

$$\begin{pmatrix} 1 & 1 & \ldots & 1 & 1 \\ (p-1) & (p-2) & \ldots & 2 & 1 \\ (p-1)^2 & (p-2)^2 & \ldots & 2^2 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (p-1)^{p-2} & (p-2)^{p-2} & \ldots & 2^{p-2} & 1 \end{pmatrix} \begin{pmatrix} -S_0 \\ S_1 \\ -S_2 \\ \vdots \\ S_{p-2} \end{pmatrix} =^p \begin{pmatrix} B_0 \\ B_1 \\ B_2 \\ \vdots \\ B_{p-2} \end{pmatrix}. \tag{8}$$

As an immediate consequence of Theorem 2.3, we obtain the following "matrix" reformulation of Kurepa's hypothesis.

Theorem 2.4. *The following statements are equivalent:*

(i) Kurepa's hypothesis holds;

(ii) for each odd prime p there holds

$$\begin{pmatrix} 1 & (p-1)^{p-2} & (p-1)^{p-3} & \dots & (p-1) \\ 1 & (p-2)^{p-2} & (p-2)^{p-3} & \dots & (p-2) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 2^{p-2} & 2^{p-3} & \ddots & 2 \\ 1 & 1 & 1 & \dots & 1 \end{pmatrix} \begin{pmatrix} B_0 \\ B_1 \\ B_2 \\ \vdots \\ B_{p-2} \end{pmatrix} \neq^p \begin{pmatrix} S_0 \\ -S_1 \\ S_2 \\ \vdots \\ -S_{p-2} \end{pmatrix};$$

(iii) for each odd prime p there holds

$$\begin{pmatrix} 1 & 1 & \dots & 1 & 1 \\ (p-1) & (p-2) & \dots & 2 & 1 \\ (p-1)^2 & (p-2)^2 & \dots & 2^2 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (p-1)^{p-2} & (p-2)^{p-2} & \dots & 2^{p-2} & 1 \end{pmatrix} \begin{pmatrix} -S_0 \\ S_1 \\ -S_2 \\ \vdots \\ S_{p-2} \end{pmatrix} \neq^p \begin{pmatrix} B_0 \\ B_1 \\ B_2 \\ \vdots \\ B_{p-2} \end{pmatrix}.$$

Theorems 2.3 and 2.4 and the fact that the square $(p-1) \times (p-1)$ matrices on the left hand side of the equalities (7) and (8) are the Vandermonde-like matrices justify the following definition.

Definition 2.5. *Let p be any odd prime. Then the matrices V_p and C_p defined as*

$$V_p = \begin{pmatrix} 1 & (p-1)^{p-2} & (p-1)^{p-3} & \dots & (p-1) \\ 1 & (p-2)^{p-2} & (p-2)^{p-3} & \dots & (p-2) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 2^{p-2} & 2^{p-3} & \ddots & 2 \\ 1 & 1 & 1 & \dots & 1 \end{pmatrix}$$

and

$$C_p = \begin{pmatrix} 1 & 1 & \dots & 1 & 1 \\ (p-1) & (p-2) & \dots & 2 & 1 \\ (p-1)^2 & (p-2)^2 & \dots & 2^2 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (p-1)^{p-2} & (p-2)^{p-2} & \dots & 2^{p-2} & 1 \end{pmatrix}$$

are called the Kurepa-Vandermonde matrices. Furthermore, the values of their determinants $\det(V_p)$ *and* $\det(C_p)$ *in the field* $\mathbb{F}_p$*, i.e.,* $\det(V_p) \pmod p$ *and* $\det(C_p) \pmod p$*, are called the Kurepa-Vandermonde determinants.*

Recall that the class number of an algebraic number field is by definition the order of the ideal class group of its ring of integers. We also prove the following result concerning the values of the Kurepa-Vandermonde determinants $\det(V_p)$ and $\det(C_p)$.

Theorem 2.6. *Let p be any odd prime. Then the Kurepa-Vandermonde matrices V_p and C_p satisfy the following inverse relation in the field $\mathbb{F}_p$:*

$$V_p \cdot C_p =^p -I_{p-1}, \tag{9}$$

where I_{p-1} is the identity matrix of order $p-1$. In other words, $C_p =^p -(V_p)^{-1}$ in the field $\mathbb{F}_p$.

Furthermore,

$$\det(V_p) = (-1)^{(p-3)(p-2)/2} \det(C_p) = -\prod_{i=1}^{p-2} (i!), \tag{10}$$

$$\det(V_p) \equiv (-1)^{(p-3)(p-2)/2} \det(C_p) \equiv (-1)^{(p^2-1)/8} \left(\frac{p-1}{2}\right)! \pmod{p} \tag{11}$$

and

$$(\det(V_p))^2 \equiv (\det(C_p))^2 \equiv (-1)^{(p+1)/2} \pmod{p}. \tag{12}$$

In particular, if $p \equiv 3 (\mathrm{mod}\ 4)$, *then*

$$\det(V_p) \equiv (-1)^{(p-3)(p-2)/2} \det(C_p) \equiv (-1)^{(p^2-1)/8+(h(-p)+1)/2} \pmod{p}, \tag{13}$$

where $h(-p)$ *is the class number of the imaginary quadratic field* $\mathbb{Q}(\sqrt{-p})$.

3. Proof of Theorems 2.3 and 2.6

Proof of Theorem 2.3 is based on the following result involving the Bell numbers B_n and the derangement numbers S_n established in 2011 by Z.-W. Sun and D. Zagier [28].

Lemma 3.1. (*[28, Theorem 1.1]*). *Let* m *be a positive integer and let* p *be a prime not dividing* m. *Then*

$$\sum_{k=1}^{p-1} \frac{B_k}{(-m)^k} \equiv (-1)^{m-1} S_{m-1} \pmod{p}. \tag{14}$$

The following result is also known.

Lemma 3.2. (see, e.g., [28, Corollary 1.3]). *If* p *is a prime then*

$$B_{p-1} - 1 \equiv S_{p-1} \pmod{p}. \tag{15}$$

Proof. [Proof of Theorem 2.3] First observe that by Fermat little theorem,

$$\begin{aligned}
\sum_{k=1}^{p-1} (p-i)^{p-k}(p-j)^{k-1} &\equiv \sum_{k=1}^{p-1} \left(\frac{p-j}{p-i}\right)^{k-1} \pmod{p} \\
&\equiv \begin{cases} p-1 \pmod{p} & \text{if } i = j; \\ \frac{\left(\frac{p-j}{p-i}\right)^{p-1}-1}{\frac{p-j}{p-i}-1} \pmod{p} & \text{if } 1 \le i \ne j \le p-1 \end{cases} \\
&\equiv \begin{cases} -1 \pmod{p} & \text{if } i = j; \\ 0 \pmod{p} & \text{if } 1 \le i \ne j \le p-1. \end{cases}
\end{aligned}$$

The above congruence shows that for the square $(p-1) \times (p-1)$ matrices $V_p = \left((p-i)^{p-j}\right)_{1 \le i \le p-1}^{1 \le j \le p-1}$ and $C_p = \left((p-j)^{i-1}\right)_{1 \le i \le p-1}^{1 \le j \le p-1}$ from the left hand sides of the equalities (7) and (8), respectively, we have $V_p \cdot C_p =^p -I_{p-1}$ in the field $\mathbb{F}_p$, where I_{p-1} is the identity matrix of order $p-1$. This shows that $C_p =^p -V_p^{-1}$ in the field $\mathbb{F}_p$, and therefore, the equalities (7) and (8) are equivalent.

Now suppose that an odd prime p is a counterexample to Kurepa's hypothesis. As the equalities (7) and (8) are equivalent, it suffices to prove the equality (7). The equivalence $(i) \Leftrightarrow (ii)$ of Proposition 2.1 yields

$$B_{p-1} \equiv 1 \pmod{p}. \tag{16}$$

Using the congruence (14) of Lemma 3.1 and applying Fermat little theorem, we find that for each $m = 1, 2, \ldots, p-1$,

$$\begin{aligned}
\sum_{k=0}^{p-2} \frac{B_k}{(-m)^k} &\equiv (-1)^{m-1} S_{m-1} + B_0 - \frac{B_{p-1}}{(-m)^{p-1}} \pmod{p} \\
&\equiv (-1)^{m-1} S_{m-1} + B_0 - B_{p-1} \pmod{p}. \qquad (17)
\end{aligned}$$

Since by Fermat little theorem, $1/(-m)^k \equiv 1/(p-m)^k \equiv (p-m)^{p-1-k} (\mathrm{mod}\ p)$ for all pairs (m,k) with $1 \leq m \leq p-1$ and $0 \leq k \leq p-2$, then substituting $B_0 = 1$ the congruence (17) becomes

$$\sum_{k=0}^{p-2} (p-m)^{p-1-k} B_k \equiv (-1)^{m-1} S_{m-1} + 1 - B_{p-1} \pmod{p},\ m = 1, 2, \ldots, p-1. \tag{18}$$

Substituting the congruence (16) into (18) gives

$$\sum_{k=0}^{p-2} (p-m)^{p-1-k} B_k \equiv (-1)^{m-1} S_{m-1} \pmod{p},\ \text{for each } m = 1, 2, \ldots, p-1. \tag{19}$$

Finally, observe that the set of $p-1$ congruences given by (19) is equivalent with the matrix equality (7) in the field $\mathbb{F}_p$.

Conversely, suppose that the matrix equality (7) in the field $\mathbb{F}_p$ is satisfied for some odd prime p. Then the first element of the matrix product on the left hand side of the equality (7) is equal to

$$\sum_{k=0}^{p-2} (p-1)^{p-1-k} B_k,$$

whence by (7) we have

$$\sum_{k=1}^{p-1} (p-1)^{p-1-k} B_{k-1} \equiv S_0 = 1 \pmod{p}. \tag{20}$$

Furthermore, the congruence (18) for $m = 1$ yields

$$\sum_{k=0}^{p-2} (p-1)^{p-1-k} B_k \equiv S_0 + 1 - B_{p-1} = 2 - B_{p-1} \pmod{p}. \tag{21}$$

Now comparing the congruences (20) and (21) gives

$$B_{p-1} \equiv 1 \pmod{p}. \tag{22}$$

In view of the equivalence $(i) \Leftrightarrow (ii)$ of Proposition 2.1, the congruence (22) shows that a prime p is a counterexample to Kurepa's hypothesis. This completes the proof of Theorem 2.3. □

Proof. [Proof of Theorem 2.6] The equality (9) is proved at the beginning of the proof of Theorem 2.3.

Notice that the $(p-1) \times (p-1)$ Kurepa-Vandermonde matrix V_p on the left hand side of (7) is a Vandermonde-type matrix. Namely, interchanging the jth column and the $(p+1-j)$th column of V_p for each $j = 2, 3, \ldots, (p-1)/2$ (the first column of V_p remains fixed), the matrix V_p becomes the Vandermonde matrix $V_p' = \left((p-i)^j\right)_{1 \leq i \leq p-1}^{0 \leq j \leq p-2}$. Hence,

$$\begin{aligned}
\det(V_p) &= (-1)^{(p-3)/2} \det(V_p') = (-1)^{(p-3)/2} \prod_{1 \leq i < j \leq p-1} ((p-j) - (p-i)) \\
&= (-1)^{(p-3)/2} \prod_{1 \leq i < j \leq p-1} (i-j) = (-1)^{(p-3)/2} (-1)^{\binom{p-1}{2}} \prod_{1 \leq i < j \leq p-1} (j-i) \quad (23) \\
&= (-1)^{(p^2-1)/2-p} \prod_{i=1}^{p-2} \prod_{j=i+1}^{p-1} (j-i) = -\prod_{i=1}^{p-2} (p-1-i)! = -\prod_{i=1}^{p-2} i! \\
&= -\left(\frac{p-1}{2}\right)! \prod_{j=1}^{(p-3)/2} (j!(p-j-1)!).
\end{aligned}$$

Notice that the matrix C_p can be obtained from the transposition V_p^T of the matrix V_p after $(p-3)+(p-2)+\cdots+1=(p-3)(p-2)/2$ suitable interchanges of its rows. This together with the equality (23) (in the third row) implies that

$$\det(V_p)=(-1)^{(p-3)(p-2)/2}\det(C_p)=-\prod_{i=1}^{p-2}(i!),$$

which is in fact, the equality (10).

In view of (10), clearly it suffices to prove only the congruences (11)–(13) concerning the determinant $\det(V_p)$.

Notice that using Wilson theorem, for each $j=1,2,\ldots,(p-3)/2$ we find that

$$\begin{aligned} j!(p-j-1)! &\equiv ((-1)^j(p-1)(p-2)\cdots(p-j))(p-j-1)! \pmod p \\ &= (p-1)!(-1)^j\equiv(-1)^{j+1} \pmod p. \end{aligned} \tag{24}$$

Substituting (24) in (23), we obtain

$$\begin{aligned} \det(V_p) &\equiv \left(\frac{p-1}{2}\right)!(-1)^{1+\sum_{j=1}^{(p-3)/2}(j+1)} \pmod p \\ &= (-1)^{(p^2-1)/8}\left(\frac{p-1}{2}\right)! \pmod p, \end{aligned} \tag{25}$$

which implies the congruence (11).

If p is a prime such that $p\equiv 3(\text{mod } 4)$, then by a congruence of Mordell [20], we have

$$\left(\frac{p-1}{2}\right)!\equiv(-1)^{(h(-p)+1)/2} \pmod p, \tag{26}$$

where $h(-p)$ is the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$. Substituting (26) into (25) gives the congruence (13).

Since

$$\left(\frac{p-1}{2}\right)!=\prod_{i=(p+1)/2}^{p-1}(p-i)\equiv(-1)^{(p-1)/2}\prod_{i=(p+1)/2}^{p-1}i \pmod p,$$

we have

$$\begin{aligned} \left(\left(\frac{p-1}{2}\right)!\right)^2 &= \left(\frac{p-1}{2}\right)!\cdot\left(\frac{p-1}{2}\right)! \\ &\equiv (-1)^{(p-1)/2}(p-1)!\equiv(-1)^{(p+1)/2} \pmod p. \end{aligned} \tag{27}$$

The congruences (25) and (27) immediately yield

$$(\det(V_p))^2\equiv\left(\left(\frac{p-1}{2}\right)!\right)^2\equiv(-1)^{(p+1)/2} \pmod p.$$

This proves (12), and the proof is completed. □

References

[1] D. Barsky and B. Benzaghou, Nombres de Bell et somme de factorielles, J. Théor. Nombres Bordeaux 16 (2004) 1–17.

[2] D. Barsky and B. Benzaghou, Erratum to the article "Nombres de Bell et somme de factorielles", J. Théor. Nombres Bordeaux 23 (2011) 527–527.

[3] L. Carlitz, A note on the left factorial function, Math. Balkanica 5:6 (1975) 37–42.

[4] S.R. Finch, Mathematical Constants, Cambridge University Press, Cambridge, 2003.

[5] Y. Gallot, yves.gallot.pagesperso-orange.fr/papers/lfact.html

[6] R. Graham, D. Knuth and O. Patashnik, Concrete Mathematics: A Foundation for Computer Science, Second Edition, Addison-Wesley, 1989.

[7] R. Guy, Unsolved problems in number theory, Springer-Verlag, 1981.

[8] A. Ivić and Ž. Mijajlović, On Kurepa's Problems in Number Theory, Publ. Inst. Math. (N.S.) 57 (71) (1995) 19–28; available at arXiv:math.NT/0312202, 2003.

[9] P. Jobling, https://groups.yahoo.com/neo/groups/primeform/conversations/topics/5095

[10] B.C. Kellner, Some remarks on Kurepa's left factorial, arXiv:math/0410477v1 [mathNT], 2004.

[11] Lj.D.R. Kočinac, The centennial of Djuro Kurepa, III Workshop on Coverings, Selections and Games in Topology, Vrnjačka Banja, Serbia, April 2007.

[12] Dj. Kurepa, On the left factorial function $!n$, Math. Balkanica 1 (1971) 147–153.

[13] R. Meštrović, A search for primes p such that the Euler number E_{p-3} is divisible by p, Math. Comp. 83 (2014) 2967–2976; available at arXiv:1212.3602v1 [math.NT], 2012.

[14] R. Meštrović, Variations of Kurepa's left factorial hypothesis, preprint arXiv:1312.7037v2 [mathNT], 2014; the first version: arXiv:1312.7037v1 [mathNT], 2014.

[15] R. Meštrović, A linear algebra formulation of Kurepa's hypothesis, in preparation.

[16] Ž. Mijajlović, On some formulas involving $!n$ and the verification of the $!n$-hypothesis by use of computers, Publ. Inst. Math. (N.S.) 47 (61) (1990) 24–32.

[17] Ž. Mijajlović, Djuro Kurepa (1907 – 1993), Publ. Inst. Math. (N.S.) 57 (71) (1995) 13–18.

[18] G.V. Milovanović, A sequence of Kurepa's functions, Sci. Rev. Ser. Eng. No. 19–20 (1996) 137–146.

[19] G.V. Milovanović and A. Petojević, Generalized factorial function, numbers and polynomials and related problems, Math. Balkanica (N.S.) 16 (No. 1–4) (2002) 113–130.

[20] L.J. Mordell, The congruence $((p-1)/2)! \equiv \pm 1 (\mathrm{mod}\ p)$, Amer. Math. Monthly 68 (1961) 145–146.

[21] A. Petojević, On Kurepa's hypothesis for left factorial, Filomat 12 (1) (1998) 29–37.

[22] A. Petojević, The function ${}_vM_m(s;a,z)$ and some well-known sequences, J. Integer Seq. 5 (2002) Article 02.1.7, 16 pages.

[23] A. Petojević, M. Žižović, and S. Cvejić, Difference equations and new equivalents of the Kurepa hypothesis, Math. Morav. 3 (1999) 39–42.

[24] D.V. Slavić, On the left factorial function of the complex argument, Math. Balkanica 3 (1973).

[25] N.J.A. Sloane, The-On-Line Encyclopedia of Integer Sequences, http://www.research.att.com/~njas/sequences/

[26] J. Stanković, Über einige Relationen zwischen Fakultäten und den linken Fakultäten, Math. Balkanica 3 (1973) 488–497.

[27] J. Stanković and M. Žižović, Noch einige Relationen zwischen den Fakultäten und den linken Fakultäten, Math. Balkanica 4 (1974) 555–559.

[28] Z.-W. Sun and D. Zagier, On a curious property of Bell numbers, Bull. Austral. Math. Soc. 84 (2011) 153–158.

[29] B. Sury, The Prime Ordeal, manuscript available at http://ias.ac.in/resonance/Volumes/13/09/0866-0881.pdf, 2008.

[30] Z. Šami, On the M-hypothesis of Dj. Kurepa, Math. Balkanica 4 (1974) 530–532.

[31] M. Tatarević, Searching for a counterexample to the Kurepa's left factorial hypothesis ($p < 10^9$), available at http://mtatar.wordpress.com/2011/07/30/kurepa/

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