PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série tome 47 (61), 1990, 24–32

ON SOME FORMULAS INVOLVING $!n$ AND THE VERIFICATION OF THE $!n$-HYPOTHESIS BY USE OF COMPUTERS

Ž. Mijajlović

Abstract. Kurepa's hypothesis for $!n$ is verified for all $n < 311009$. Some new equivalents to the hypothesis are also found.

0. Introduction

Kurepa introduced in [**2**] the notion of the left factorial in the following way:

$$!n = \sum_{i=0}^{n-1} i!, \qquad n \in N,$$

where N is the set of nonnegative integers. In the same paper Kurepa asked if

$$\forall n \in N \, (!n, n!) = 2 \tag{KH}$$

Here (a, b) denotes the greatest common divisor of integers a and b. This conjecture is still an open problem in number theory. There are several results which may speak in the behalf of the hypothesis. For example, Kurepa showed in [**3**] that there are infinitely many $n \in N$ for which KH is true. Also, the conjecture is verified by use of computers (Slavić for $n \leq 1000$, and Wagstaff extended the calculation for $n \leq 50000$). Finally there are several statements equivalent to the hypothesis ([**2**], [**5**], [**6**]). One of the most interesting is the following statement, which also belongs to Kurepa (see [**2**]):

$$\forall n > 2 \;\; !n \neq 0 \mod n$$

We shall call this statement also KH. This formulation of KH appears as the open problem B44 in [**1**]. The aim of this paper is to state some new propositions equivalent to KH, and to exhibit a method for the verification of KH for reasonable large n. Implementing this method on computers we verified KH for all $n < 311009$.

AMS Subject Classification (1985): Primary 10-04, 10 A 10, Secondary 10 A 05, 10 A 25

1. Some new equivalents

In [2] it was shown that KH can be reduced to primes, i.e. that KH is equivalent to

$$\forall p \in P \,(p > 2 \Rightarrow (!p, p) = 1) \tag{PH}$$

where P is the set of all primes. If p is a prime and PH is true for all primes $\leq p$ then KH is true for all integers $n \leq p$. This statement easily follows from the fact that all primes which divide $n!$ are $\leq n$. This observation is the key point in our approach to the verification of KH by means of computers.

If p is a prime, let GF(p) be the Galois field of p elements.

Lemma 1.1. *If p is a prime ≥ 3 then in* GF(p) *we have*

$$!p = \sum_{k=0}^{p-1} (-1)^{k+1}/k! \tag{1-1}$$

$$!p = \sum_{k=0}^{p-1} (-1)^{k}(k+1)(k+2)\dots(p-1) \tag{1-2}$$

Proof. All operations in this proof are the operations of the field GF(p). By Wilson Theorem we have

$$(p-1)! = -1. \tag{1-3}$$

Further, for $0 \leq k \leq p-1$,

$$(p-1)! = (p-k-1)!(p-k)(p-(k-1))\dots(p-1). \tag{1-4}$$

Observing that in GF(p) $p = 0$, we have

$$(p-1)! = (p-k-1)!k!(-1)^k. \tag{1-5}$$

Therefore,

$$\begin{aligned} !p &= \sum_{k=0}^{p-1} k! \\ &= \sum_{k=0}^{p-1} (-1)^{k+1}/(p-k-1)!, \qquad \text{using the substitution } j = p-k, \\ &= \sum_{j=1}^{p} (-1)^{p-j+1}/(j-1)! \\ &= \sum_{j=0}^{p-1} (-1)^{j+1}/j!. \end{aligned}$$

Thus (1-1) holds. Further, by this identity we have

$$\begin{aligned} !p &= \sum_{k=0}^{p-1}(-1)^{k+1}/k! \\ &= \sum_{k=0}^{p-1}\frac{(-1)^{k+1}}{(p-1)!}(k+1)(k+2)\dots(p-1), \qquad \text{by Wilson Theorem,} \\ &= \sum_{k=0}^{p-1}(-1)^{k}(k+1)(k+2)\dots(p-1) \\ &= 1\cdot 2\cdot 3\dots(p-1) - 2\cdot 3\dots(p-1) + \dots + (-1)^{p-2}(p-1) + (-1)^{p-1}, \end{aligned}$$

and this proves (1-2). ♢

Corollary 1.2. KH *is equivalent to*:
For all primes p, GF(p) *verifies* $\sum_{k=0}^{p-1}(-1)^{k+1}/k! \neq 0$.

Corollary 1.3. KH *is equivalent to any of the following statements*

1. *For all primes p,* GF(p) *verifies* $\sum_{k=0}^{p-1}(-1)^{k}(k+1)(k+2)\dots(p-1) \neq 0$.
2. *For all primes p,* $\sum_{k=0}^{p-1}(-1)^{k}(k+1)(k+2)\dots(p-1) \neq 0 \mod p$.

Corollary 1.4. KH *is equivalent to any of the following statements*

1. *For all primes p,* GF(p) *verifies* $\sum_{k=0}^{p-1}\binom{p-1}{k}(k+1)(k+2)\dots(p-1) \neq 0$
2. *For all primes p,* $\sum_{k=0}^{p-1}\binom{p-1}{k}(k+1)(k+2)\dots(p-1) \neq 0 \mod p$.

The last corollary follows from the Corollary 1.3. and the well-known relation $\binom{p-1}{k} = (-1)^k \mod p$ for all primes p (which is in fact an immediate consequence of (1-5)).

2. Recurrent formulas

First we introduce some notation. If m, n are integers, then by $r = \mathrm{rest}(m,n)$ we shall denote the reminder obtained from division of m by n. Further, by $\mathcal{Z}_n$ we denote the ring $(Z_n, +_n, \cdot_n, 0, 1)$, where $Z_n = \{0,1,2,\dots,n-1\}$. Let r_n be the sequence defined by $r_n = \mathrm{rest}(!n, n)$, $n \in N$. In this section we shall derive some recurrent relations in $\mathcal{Z}_n$ which shall enable us to compute r_n.

Lemma 2.1. *If q is a prime and s_i is a sequence defined in* GF(q) *by regressive induction*

$$\begin{aligned} s_{q-1} &= 0 \\ s_i &= 1 + is_{i+1}, \qquad i = q-2, q-3, \dots, 1 \end{aligned} \tag{2-1}$$

then $r_q = s_1$.

Proof. We have

$$!q = 1 + 1 \cdot (1 + 2(1 + 3(1 + \ldots + (1 + (q-3)(1 + (q-2)q)) \ldots)$$

Therefore, taking $u_i = 1 + i(1 + (i+1)(1 + \ldots (1 + (q-2)q)) \ldots)$, $i = q-2, \ldots, 1$, $u_{q-1} = q$, we obtain $u_i = 1 + iu_{i+1}$, $i = q-2, q-3, \ldots, 1$, and $!q = u_1$. If we take $s_i = \mathrm{rest}(u_i, q)$, then s_i satisfies (2-1) in $\mathrm{GF}(q)$. ♢

Lemma 2.2. *If q is a prime, and t_i is a sequence defined in* $\mathrm{GF}(q)$ *by induction in the following way*:

$$\begin{aligned} t_1 &= 0 \\ t_i &= (-1)^i + it_{i-1}, \qquad i = 2, 3, \ldots, q-1 \end{aligned} \tag{2-2}$$

then $r_q = t_{q-1}$.

Proof. By Lemma 1.1 we have in $\mathrm{GF}(q)$

$$\begin{aligned} !q &= \sum_{k=0}^{q-1} (-1)^k (k+1)(k+2) \ldots (q-1) \\ &= 1 \cdot 2 \cdot 3 \ldots (q-1) - 2 \cdot 3 \cdot \ldots (q-1) + \ldots (-1)^{q-2} + (-1)^{q-1} \\ &= (\ldots (1-1)2 + 1)3 - 1)4 + 1) \ldots)(q-2) + (-1)^{q-2}(q-1) + (-1)^{q-1} \end{aligned}$$

Thus taking

$$t_i = (\ldots(((1-1)2 + 1)3 - 1)4 + 1) \ldots)i + (-1)^i, \qquad i = 1, 2, \ldots, q-2,$$

we obtain (2-2). ♢

Lemma 2.3. *If q is a prime, and v_i is a sequence defined in* $\mathrm{GF}(q)$ *by*

$$\begin{aligned} v_1 &= 0 \\ v_j &= 1 - jv_{j+1}, \qquad j = 1, 2, \ldots, q-2, \end{aligned}$$

then $r_q = v_{q-1}$.

Proof. For the sequence s_i in Lemma 2.1. we have

$$s_{q-i} = 1 + (q-i)s_{q-i+1},$$

so for $v_i = s_{q-i}$ we have (observe that $q = 0$ in $\mathrm{GF}(q)$:

$$\begin{aligned} v_1 &= 0 \\ v_j &= 1 - jv_{j+1}, \qquad j = 1, 2, 3, \ldots q-1, \\ v_{q-1} &= s_1 = r_q. \end{aligned}$$

$\diamondsuit$

Now we shall consider some other relations for r_n.

LEMMA 2.4. $m|n \Rightarrow r_n = r_m \mod m$.

Proof. Suppose $m|n$. First we have $!n = r_n \mod n$, so as $m|n$, $!n = r_n \mod m$. As $\mathrm{rest}(!n, m) = \mathrm{rest}(!m, m) = r_m$, and $!n = \mathrm{rest}(!n, m) \mod m$ it follows $r_n = r_m \mod m$. $\diamondsuit$

COROLLARY 2.5. *If $m|n$ and $r_n \leq m$ then $r_n = r_m$.*

Suppose $n = n_1 n_2 \dots n_k$ where $(n_i, n_j) = 1$ for $1 \leq i < j \leq k$. Then by Lemma 2.4, $r_n = r_{n_i} \mod n_i$, $1 \leq i \leq k$. Therefore, as $r_n < n$, by Chinese Reminder Theorem r_n is the least nonnegative solution of the sistem of congruences $x = r_{n_i} \mod n_i$, $1 \leq i \leq k$.

Further, if $r_n = 0$ and p is a prime dividing n then by Lemma 2.4 $r_p = 0$. This yields a proof of the equivalence KH $\Leftrightarrow$ PH.

By the above remarks, the number r_n is uniquely determined by the prime decomposition $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_3^{\alpha_3}$. Namely, in this case there is an isomorphism

$$\theta : \mathcal{Z}_{p_1^{\alpha_1}} \times \mathcal{Z}_{p_2^{\alpha_2}} \times \dots \mathcal{Z}_{p_k^{\alpha_k}} \longrightarrow \mathcal{Z}_n,$$

where for $x \in Z_n$, $x_i \in Z_{p_i^{\alpha_i}}$, $1 \leq i \leq k$,

$$x = \theta(x_1, x_2, \dots, x_k) \quad \text{iff} \quad \text{for all } 1 \leq i \leq k, \quad x = x_i \mod p_i^{\alpha_i}.$$

Thus r_n can be computed by

$$r_n = \theta(r_{p_1^{\alpha_1}}, \dots, r_{p_k^{\alpha_k}}).$$

3. The Second Kurepa hypothesis

In [**2**] Kurepa also conjectured the following hypothesis:

(KH2) *The relation $m^2|!n$, except $2^2|!3$, does not have solutions in integers greater than* 1.

Obviously KH2 is equivalent to to the statement that $!n$ is square-free. Thus we shall consider KH2 only for primes m. If p is a prime and $n \geq p$ then $p^2|!p$ implies $p|!p$, therefore we have immediately:

PROPOSITION 3.1. KH *implies that for any m there are at most finitely many n such that $m^2|n$.*

Let KH(m) denote the Kurepa hypothesis for all integers bellow m i.e. KH(m) is the formula

$$\forall n \leq m \ \ (n > 2 \Rightarrow !n \neq 0 \mod n)$$

Therefore, KH $\Leftrightarrow \forall m$ KH(m). Further, let KH2(m) denote the formula

$$\forall k < m\, \forall n < k \ \ (1 < k \wedge 3 < n \Rightarrow \mathrm{rest}(!n, k^2) \neq 0).$$

By above remarks we have immediately the following statement:

Proposition 3.2. KH $\wedge\, \forall m$ KH2$(m) \Rightarrow$ KH2.

As an refinement of the last proposition we have the following. Assuming KH is true it suffices to check if for $r_n^2 = \mathrm{rest}(!n, p^2)$

$$r_n^2 \neq 0, \quad \text{for} \ \ n < p \tag{3-1}$$

to conclude that there is no n such that $p^2|!n$. Also, if (3-1) is verified for all primes $p \leq m_0$ then for all $m \leq m_0$ there is no n such that $m^2|!n$. Kurepa stated in [**2**] that, except $2^2|!3$, for $m = 2, 3, 4, 5, 6, 7, 8$ for no n, $m^2|!n$. Using the above observation we approved this statement for first 200 primes, so KH2(m) is true for $m \leq 1223$. In this computation we can use similar recurrent formulas as in Lemma 2.1. Namely it is easy to see that for the sequence s_i defined in Z_{p^2} by regressive induction

$$\begin{aligned} s_{n-1} &= n \\ s_i &= 1 + i \cdot s_{i+1}, \quad i = n-2, n-3, \ldots, 1, \end{aligned} \tag{3-2}$$

we have $r_n^2 = s_1$.

4. Program implementation

Using formulas developed in previous sections, we implemented computer programs for verifying KH and KH2. All programs are written in FORTRAN 77 for transputer station based on three transputers T800. Some of the routines were implemented in parallel version of FORTRAN 77 (3L Parallel FORTRAN) using the advantage of parallel computing abilities of processors T800.

4.1. *Computer verification of* KH. In fact we were verifying KH(m) for $m \leq m_0$, where m_0 is the given bound. The first part of the program is used to generate the sequence of first i_0 primes p_i, $1 \leq i \leq i_0$. In the main part of the program KH(p_i) is checked for $i \leq i_0$. As for $i_0 = 26880$, for which $p_{i_0} = 311009$, for no $i \leq i_0$ $r_{p_i} = 0$, it follows (see the beginning of Section 1) that KH(n) is true for all $n \leq 311009$; thus in our case $m_0 = 311009$.

In the computation of r_p we were using recurrent formulas (2-1), therefore the program code of this part of the program looks as

This facility belongs to the Mathematical Faculty of the Faculties of Sciences, University of Belgrade

```
      DO 1001 J=IP,L
      Q=P(J)
      KNOD=Q
      QD=Q
      DO 1002 IL=Q-2,1,-1
1002  KNOD=DMOD(DBLE(1+IL*KNOD),QD)
      WRITE(2,405) J,Q,KNOD
      IF (KNOD.EQ.0) THEN
      STOP
      ENDIF
1001  CONTINUE
C     P(J) is the sequence of primes
C     KNOD and QD are DOUBLE PRECISION variables
C     The value of KNOD after the loop 1002 is r_Q
```

Some refinements are used in the program. In order to make possible computation in several sessions, the program is written so that $\mathrm{KH}(p_i)$ can be verified in an interval $i_1 \le i \le i_2$ (in the above program $i_1 =$ `IP`, and $i_2 =$ `L`). If $i \le 4792$ then $p_i \le 46337$ so `1+IL*KNOD` in the above listing does not exceed the `INTEGER` bound in FORTRAN 77, and `DBLE` can be omitted in the line 1001 of the listing, and variables `KNOD, QD` can be replaced by the `INTEGER` variable Q. Therefore, for small values of p_i ($p_i \le 46337$) only `INTEGER` varaibles can be used, thus the program can be speeded up for several times (and then it takes only several minutes to check KH(46337)).

Further, the whole program is written as a transputer application divided into k tasks (in our case $k = 3$) so that each processor of the transputer station can execute in parallel a task. The task T_j is used to verify $\mathrm{KH}(p_i)$ for $i = j \mod k$, $i \le i_0$. From the program code we see that the number of arithmetical operations needed for the computation of r_p is $4p$. Thus the total number of arithmetical operations used in the verification of $\mathrm{KH}(x)$ is

$$A = \sum_{p \le x} 4p \tag{4-2}$$

where p in the sum runs over primes. Using Stieltjes integral, we obtain

$$A = 4\int_2^x x d\pi(x) = 4x\pi(x)|_2^x - 4\int_2^x \pi(x)dx \sim 4x\pi(x) \sim \frac{4x^2}{\ln x},$$

where $\pi(x)$ is the number of primes $\le x$. Hence, we have the following asymptotic formula

$$A \sim \frac{4x^2}{\ln x} \tag{4-3}$$

If k transputers are used (we call a such configuration a k-farm), and if τ is an average execution time interval of an arithmetical operation, then

$$A_k(x) = \frac{4x^2\tau}{k \cdot \ln x} \tag{4-4}$$

is the total time used for the above computation. In order to find the efficiency of k-farms in respect to one-transputer station, we compare $A_k(x)$ and $A_1(y)$ for the same time interval, i.e. for given y we determine x from

$$\frac{4x^2\tau}{k \cdot \ln x} = \frac{4y^2\tau}{\ln y}.$$

Therefore, $x = \sqrt{k}\sqrt{\ln x / \ln y} \cdot y$. From this equation it follows that the efficiency of a k-farm in the verification of KH(y) is $e(y) = \sqrt{k}\sqrt{\ln x / \ln y} > \sqrt{k}$. For fixed k it is easy to see that $\lim_{y\to\infty} \sqrt{\ln x / \ln y} = 1$, so for large intervals the efficiency of a k-farm is asymptotically equal to $\sqrt{k}$. This means that if one transputer in a given time interval verifies KH(x), then a k-farm in the same time interval verifies KH$(x\sqrt{k})$.

Prime factorization table of $!n$

n	$!n$	Factorization
1	1	1
2	2	2
3	4	$2 \cdot 2$
4	10	$2 \cdot 5$
5	34	$2 \cdot 17$
6	154	$2 \cdot 7 \cdot 11$
7	874	$2 \cdot 19 \cdot 23$
8	5914	$2 \cdot 2957$
9	46234	$2 \cdot 23117$
10	409114	$2 \cdot 204557$
11	4037914	$2 \cdot 2018957$
12	43954714	$2 \cdot 19 \cdot 31 \cdot 37313$
13	522956314	$2 \cdot 881 \cdot 296797$
14	6749977114	$2 \cdot 227 \cdot 379 \cdot 39229$
15	93928268314	$2 \cdot 75437 \cdot 622561$
16	1401602636314	$2 \cdot 19 \cdot 41 \cdot 491 \cdot 1832213$
17	22324392252 4314	$2 \cdot 127399 \cdot 87616043$
$*18$	378011820620314	$2 \cdot 76753 \cdot 2462521469$
19	6780385526348314	$2 \cdot 197 \cdot 17209100320681$
20	128425485935180314	$2 \cdot 27067 \cdot 455599 \cdot 5207129$
21	2561327494111820314	$2 \cdot 500473 \cdot 2558906768309$
22	53652269665821260314	$2 \cdot 37 \cdot 317 \cdot 16823 \cdot 135954526571$
23	1177652997443428940314	$2 \cdot 6893917 \cdot 85412472868721$
24	27029669736328405580314	$2 \cdot 31 \cdot 89 \cdot 991 \cdot 1607 \cdot 3075880875779$

4.2. *Computer verification of* KH2. According to Section 3 it suffices to verify KH2(m). Using formulas (3-2) we checked KH2(m) for $m \le 1223$, so $m^2|n$ has no solutions for $m \le 1223$ and arbitrary n.

We also computed the prime decomposition of $!n$ for $n \leq 24$, see the table. As it is seen, $!n$ is squarefree for $n \leq 24$. For the prime decomposition of these numbers we used the tabulation of $!n$ in [**7**], and algorithms presented in [**4**]. These algorithms are implemented in FORTRAN 77 by M. Dražić.

REFERENCES

[**1**] R. Guy, *Unsolved Problems in Number Theory*, Springer-Verlag, 1981.

[**2**] Đ. Kurepa, *On the left factorial function*, Math. Balkan. **1** (1971), 147–153.

[**3**] Đ. Kurepa, *On some new left factorial propositions*, Math. Balkan. **4** (1974), 383–386.

[**4**] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhäuser, 1985.

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

[**6**] Z. Šami, *On the M-hypothesis of Đ. Kurepa*, Ibidem, 530–532.

[**7**] V. Vuletić, *Tabulation of the functions*: $\Gamma(n+1) = n!$, $K(n) = !n$, $r(n)$, $\nu_s(n) = \nu(s, n)$, Math. Balkan. **4** (1974), 675–706.

Matematički fakultet
Studentski trg 16
11000 Beograd, Jugoslavija

(Received 01 07 1989)
(Revised 09 09 1989)