

THE NUMBER OF PRIMES $\sum_{i=1}^n (-1)^{n-i} i!$ IS FINITE

MIODRAG ŽIVKOVIĆ

ABSTRACT. For a positive integer n let $A_{n+1} = \sum_{i=1}^n (-1)^{n-i} i!$, $!n = \sum_{i=0}^{n-1} i!$ and let $p_1 = 3612703$. The number of primes of the form A_n is finite, because if $n \geq p_1$, then A_n is divisible by p_1 . The heuristic argument is given by which there exists a prime p such that $p \mid !n$ for all large n ; a computer check however shows that this prime has to be greater than 2^{23} . The conjecture that the numbers $!n$ are squarefree is not true because $54503^2 \mid !26541$.

Let N and P denote the set of positive integers and the set of prime numbers, respectively. For integers m, n let (m, n) denote their greatest common divisor, and let $m \bmod n$ denote the remainder from division of m by n . The fact that m divides (does not divide) n is written as $m \mid n$ ($m \nmid n$). For $n \geq 2$ let

$$A_{n+1} = \sum_{i=1}^n (-1)^{n-i} i!$$

and let

$$!n = \sum_{i=1}^{n-1} i!$$

(the left factorial function was defined by Kurepa [7]). Here we consider the following three questions from [3]. Is it true that

$$(1) \quad a_p := A_p \bmod p \neq 0 \text{ for all } p \in P?$$

(This question is raised in connection with [3, Problem B43]: is it true that there are infinitely many prime numbers among A_n , $n \in N$.) Is it true that

$$(2) \quad r_p := !p \bmod p \neq 0 \text{ for all } p \in P, \quad p > 2?$$

(This is from [3, Problem B44]; an equivalent of the Kurepa hypothesis [7].) And is it true that

$$(3) \quad \text{for all } n \in N, \quad n > 3, \quad !n \text{ is squarefree?}$$

(This is also in [3, Problem B44]; the second Kurepa hypothesis [7], [9].)

According to [3, Problem B44], R. Bond claims to have proved (2); but he informed this author that he later discovered an error in the proof. Wagstaff verified that (1) and (2) are true for $n < 46340$ and $n < 50000$, respectively. The calculations were extended by Mijajlović in [9] ((2) for $p \leq 311009$), Gogić in [2] ((1) and (2) for $p < 1000000$) and Malešević in [8] ((2) for $p < 3000000$). Mijajlović proved

Received by the editor July 19, 1996 and, in revised form, January 23, 1997.
1991 *Mathematics Subject Classification*. Primary 11B83, Secondary 11K31.
Key words and phrases. Prime numbers, left factorial, divisibility.

in [9] that if $n \in N$, $p \in P$ and $2 < p \leq 1223$, then $n!$ is not divisible by p^2 . A new overview of these questions is given in [4].

For $k \in N$ let $N(k) = \{0, 1, \dots, k-1\}$ and let R_k denote the random variable with the uniform probability distribution (PD) over the set $N(k)$. The values $n! \bmod p$ and $n! \bmod p^2$, $1 \leq n < p$, might be considered the independent realizations of R_p and R_{p^2} , respectively (a more precise model could exclude a few boundary values of n). Consequently, for arbitrary $p \in P$ we can think of a_p and r_p as the realizations of R_p .

To check these assumptions, two types of chi-square statistical tests were carried out (for details see, for example, [6, Chapter 3]). The purpose of the first test was to check if given $n = p-1$ integers $z_i \in N_p$, $1 \leq i < p$, might be considered independent realizations of R_p (the interesting cases for z_i are $i!$, $!(i+1)$, and A_{i+1}). The number k is appropriately chosen and the set N_p is divided into k subsets (categories), so that z_i belongs to the category $[kz_i/p] \in N_k$, $1 \leq i < p$ (here $[x]$ denotes the integral part of the real number x). The frequencies

$$f_j = \{i, 1 \leq i < p \mid [kz_i/p] = j\}, \quad 0 \leq j < k,$$

and the expected values $n\pi_j$, $0 \leq j < k$, can be computed, where

$$\pi_j = Pr([kR_p/p] = j) = ([pi/k] - [p(i-1)/k] + \delta_{i,0} - \delta_{i,k-1})/p \simeq 1/k.$$

Here $\delta_{i,j}$ is the Kronecker symbol, equal to 1 (0) if $i = j$ ($i \neq j$). The frequencies are checked using the χ^2 statistics,

$$(4) \quad \chi^2 = \sum_{i=0}^{k-1} (f_j - n\pi_j)^2 / (n\pi_j).$$

If the value of χ^2 is large, then we can say that this experiment contradicts the uniformity of z_i , $1 \leq i < p$. The values of χ^2 are calculated with p taking values from a set of random primes (the two first primes following the randomly chosen integer from $(2^l, 2^{l+1})$, $10 \leq l \leq 23$), and with z_i equal to $i!$, $!(i+1)$, and A_{i+1} , $1 \leq i < p$, respectively. As expected, the results do not contradict the uniformity assumption. The results for the pairs of consecutive primes do look independent.

The aim of the second type of test is to check the uniformity of the distribution of a_p/p and r_p/p (when $p \in P$ varies) between the subdivisions

$$(5) \quad [i/k, (i+1)/k), \quad 0 \leq i < k,$$

of the unit interval, for some fixed k . Let z_p denote a_p or r_p . Choose some integers $a < b$ and a prime $p \in P(a, b) := \{p \in P \mid a \leq p < b\}$. For $0 \leq j < k$ compute the frequencies

$$f_j = |\{p \in P(a, b) \mid [kz_p/p] = j\}|,$$

and the category probabilities

$$\pi_j = Pr([kR_p/p] = j) \simeq 1/k.$$

Let $n = |P(a, b)|$ be the cardinality of $P(a, b)$. The PD of R_p/p over the equal intervals (5) is approximately uniform and independent of p . The values of χ^2 (4) are computed for $z_p = a_p, r_p$, and $(a, b) = (2^l, 2^{l+1})$, $10 \leq l \leq 23$ ($10 \leq l \leq 22$ when $z_p = a_p$). The results obtained do not contradict the supposed statistical model.

Using the assumptions about a_p and r_p , we see that (1) and (2) are related to the event

$$R_\infty = \bigcap_{p \in P} \{R_p \neq 0\}.$$

But according to Mertens's theorem (see [10, Theorem 3.1] for example)

$$\prod_{p \in P(2, x)} \left(1 - \frac{1}{p}\right) \simeq \frac{e^{-\gamma}}{\ln x} \quad \text{as } x \rightarrow \infty,$$

where γ is Euler's constant, so $e^{-\gamma} \simeq 0.5615$. Therefore, $Pr(R_\infty) = 0$. More precisely, we have the following asymptotic relation

$$Pr \left(\bigcap_{p \in P(x, x^\alpha)} \{R_p \neq 0\} \right) \simeq \frac{1}{\alpha}, \quad \text{as } x \rightarrow \infty.$$

This heuristic argument suggests that (1) and (2) are not true, and even more, that the number of counterexamples is infinite. The "probability" that there is a counterexample $p \in P(x, x^\alpha)$ to (1) or (2) is approximately $1 - 1/\alpha$. With the same probability of $1/2$, one counterexample to these claims might be expected in the intervals $(2^3, 2^6] = (8, 64)$, $(2^6, 2^{12}] = (64, 2048]$ and $(2^{12}, 2^{24}] = (2048, 16793216]$. The probability of finding counterexamples in $(2^n, 2^{n+1}]$ is approximately $1/(n+1)$. The complexity of the search for a counterexample $\leq x$ by the obvious algorithm is $O(x^2/\ln x)$ [9], which makes it very difficult to check (1) or (2) if, for example, $p > 2^{24}$.

The search for values $p \in P$ satisfying $p | A_p$ was performed using a simple assembler routine for an Intel 80486 microcomputer (at 100MHz) calculating a_p . After approximately 130 hours it was found that for $p = p_1 = 3612703$ we have $p | A_p$. This fact gives a solution of [3, Problem B43], because for all $n \geq p_1$ we have $p_1 | A_n$, and so A_n is not prime if $n \geq p_1$. The numbers A_n are prime for $n \in \{4, 5, 6, 7, 8, 9, 11, 16, 20, 42, 60, 62, 106, 161\}$. Keller (see [3, Problem B43]) found the last five primes from the list and checked the primality of A_n for $n \leq 336$. The necessary condition for primality

$$(6) \quad 3^{M-1} \equiv 1 \pmod{M},$$

where $M = A_n$, is not satisfied if $336 < n \leq 563$ (calculations are done using UBASIC [11]), and so the list of known primes A_n remains unchanged. By a heuristic argument it could be estimated that if $n < p_1$, then A_n is prime with the "probability" $2/n$ (its prime factors are between n and $\sqrt{A_n}$) and that the total number of primes A_n is approximately $2 \ln p_1 \simeq 30$.

The similar search for values $p \in P$ satisfying $p | !p$, approximately 600 hours long, ended without success. No counterexamples were found to (2) for $p < 2^{23}$. The files containing all the residues a_p , $p \in P(2, 2^{22})$ and r_p , $p \in P(2, 2^{23})$, can be obtained from the author on request. An excerpt from the files is given in Table 1 where the instances of a_p and r_p less than 10 or greater than $p - 10$ are listed. Here we see that the congruences $!p \equiv 8 \pmod{p}$ and $!p \equiv -7 \pmod{p}$ have no solutions $p < 2^{23}$. This means that $(!n - 8)/2$ and $!n + 7$ are not divisible by any prime less than 2^{23} ; as for A_n , it is not known whether the number of primes of those two forms is finite (of course, according to the probabilistic model, it *is*

TABLE 1. The values of a_p , $p < 2^{22}$, and r_p , $p < 2^{23}$, close to 0 or p

p	a_p	p	$p - a_p$	p	r_p	p	$p - r_p$
2	1	2	1	2	0		
3	1	3	2	3	1	3	2
5	4	5	1	5	4	5	1
7	3	7	4	7	6	7	1
11	4	11	7	11	1	13	3
17	8	13	1	19	9	17	4
31	9	17	9	31	2	23	2
41	1	19	5	37	5	67	2
43	5	23	5	41	4	71	3
47	6	37	1	163	4	113	4
67	5	71	7	197	9	139	5
79	4	109	5	277	7	227	2
157	6	131	3	373	2	349	6
191	6	197	2	467	3	2437	5
307	5	229	9	7717	7	4337	5
641	3	367	4	11813	6	10331	2
647	5	463	1	33703	9	77687	3
1109	2	691	2	2275843	3	126323	8
2741	3	983	3	3467171	5	274453	1
3559	3	1439	2			4709681	9
394249	1	11119	3				
2934901	1	16007	4				
3612703	0	22619	3				
		32833	6				
		3515839	2				

finite). The check shows that (6) is satisfied by $M = (!n - 8)/2$, $n \leq 563$ if

$$n \in \{5, 6, 7, 8, 11, 14, 15, 16, 21, 25, 48, 49, 70, 108, 111, 296^*\},$$

and that (6) is satisfied by $M = !n + 7$, $n \leq 563$ if

$$n \in \{3, 4, 5, 7, 10, 12, 20, 37, 52, 73, 149, 304^*, 540^*\}.$$

Primality of those numbers (excluding the ones with the corresponding n marked by an asterisk) is proved using UBASIC program APRT-CLE [1].

Let a be an arbitrary integer. Consider now divisibilities from [3, Problem B44], i.e. the prime powers p^k ($k \geq 1$) dividing $!n + a$ for all large n . For given $p \in P$ and $k \in N$ let

$$m(p, k) = \min \{i \in N \mid p^k \mid i!\}.$$

The number $m(p, k)$ is of course a multiple of p , and if $k \leq 3$, then $m(p, k) = (k - \delta_{p,2})p$. For all $n \geq m(p, k)$ we have

$$!n \equiv !m(p, k) \pmod{p^k}.$$

Therefore, for all $n \geq m(p, k)$

$$(7) \quad p^k \mid !n + a \quad \text{iff} \quad p^k \mid !m(p, k) + a.$$

Especially, if $p > 2$ and $k \leq 3$, then for all $n \geq kp$

$$(8) \quad p^k \mid !n + a \quad \text{iff} \quad p^k \mid !(kp) + a.$$

The case $a = -1$ is considered by Mijajlović and Keller ([3, Problem B44]). Mijajlović noted that $3 \mid !n - 1$ for $n \geq 3$, $9 \mid !n - 1$ for $n \geq 6$, and $11 \mid !n - 1$ for $n \geq 11$ (by (8) this is the consequence of $3 \mid !3 - 1$, $3^2 \mid !6 - 1$ and $11 \mid !11 - 1$). Keller found no new divisibilities of $!n - 1$ for $n < 10^6$. From Table 1 it can be seen that 3 and 11 are the only primes $p < 2^{23}$ satisfying $r_p = 1$, and therefore dividing $!n - 1$ for all large n . In Table 2 the factorizations of $!n - 1$, $n \leq 42$, (obtained using [5]) are given. The consequence of $11^2 \nmid (2 \times 11) - 1$ and $3^3 \nmid (3 \times 3) - 1$ is that $11^2 \nmid !n - 1$ for $n \geq 22$ and $3^3 \nmid !n - 1$, for $n \geq 9$. We conclude that $p^k = 3^2$ is the only repeated factor of $!n - 1$ for all large n if $p < 2^{23}$.

The case $a = 0$ is somewhat simpler. Because $r_p \neq 0$ for all $p \in P(2, 2^{23})$, there is not any $p < 2^{23}$ such that $p \mid !n$ for all large n . The other cases $-10 < a < 10$ might be considered similarly using Table 1.

The other consequence of (7) is that if for the given prime power p^k , $k \geq 1$, we are looking for all $n \in N$ such that $p^k \mid !n + a$, then it is enough to check the values of $n \leq m(p, k)$. Let l be the smallest integer satisfying $p^l \nmid !m(p, l) + a$. If $l < k$, then it is enough to check if $p^k \mid !n + a$ for $n < m(p, l) \leq m(p, k)$ ($n < p$ if $l = 1$, which is most often the case). Otherwise, if $l \geq k$, then $p^k \mid !m(p, k) + a$ and so $p^k \mid !n + a$ for all $n \geq m(p, k)$. Some repeated factors of $!n - 1$ may be seen from Table 2: $3^4 \mid !8 - 1$, $11^2 \mid !13 - 1$, $11^2 \mid !21 - 1$ and $37^2 \mid !25 - 1$. By (8) there are no other numbers $!n - 1$ divisible by 3^3 or 11^2 , because $3^3 \nmid !9 - 1$ and $11^2 \nmid !22 - 1$. In Table 3 the triads (p, n, r) are listed satisfying $r = !n \pmod p < 10$, $p \in P(2, 2^{20})$ and $n \leq 2p$, except those for which $!n < p$. We see that the only new solution of $p^2 \mid !n - 1$, $p < 2^{20}$, $n \in N$, is $41611^2 \mid !26144 - 1$. From Table 1 we see that $r_{41611} \neq 1$ and consequently $41611 \nmid !n - 1$ for $n \geq 41611$.

Table 3 contains a counterexample to (3): the relation $54503^2 \mid !26541$ shows that left factorials are not always squarefree. The existence of a counterexample also has a “probabilistic” explanation. Considering the values $!n \pmod{p^2}$, $1 \leq n \leq p$, as the independent realizations of R_{p^2} , the check of $!n \pmod{p^2} \neq 0$, $1 \leq n \leq p$, for fixed $p \in P$ corresponds to the event T_p that p independent outcomes of R_{p^2} are all different from 0. Using the inequality

$$1 - \frac{1}{n} < \left(1 - \frac{1}{n^2}\right)^n < \left(1 - \frac{1}{n}\right) / \left(1 - \frac{1}{n^2}\right),$$

which can be easily proved, we conclude that

$$Pr(T_p) = (1 - 1/p^2)^p \simeq 1 - 1/p$$

for large p . It follows that (3) and (1) have the same asymptotic “counterexample densities”.

The seemingly unexpected repetitions in Table 3 can be explained as follows. The remainders $!n \pmod{p^2}$, $p \leq n \leq 2n$, have the same remainder $\pmod p$. Therefore, if $!p \pmod p < 10$ (hence this p appears in Table 1), then with the high “probability” of $(1 - 1/p)^{p-1} \simeq e^{-1}$ there will be exactly one such entry (p, n, r) in Table 3; furthermore, with the “probability” of $\binom{p}{2} 1/p^2 (1 - 1/p)^{p-2} \simeq 0.5e^{-1}$ there will be two entries (p, n, r) and (p, n', r) with the same small remainder. Even the probability of three entries differing only in the second position is not too small,

TABLE 2. The factorizations of $!n - 1$, $n \leq 42$

n	The factorization of $!n - 1$
3	3
4	3^2
5	3×11
6	$3^2 \times 17$
7	$3^2 \times 97$
8	$3^4 \times 73$
9	$3^2 \times 11 \times 467$
10	$3^2 \times 131 \times 347$
11	$3^2 \times 11 \times 40787$
12	$3^2 \times 11 \times 443987$
13	$3^2 \times 11^2 \times 23 \times 20879$
14	$3^2 \times 11 \times 821 \times 83047$
15	$3^2 \times 11 \times 2789 \times 340183$
16	$3^2 \times 11 \times 107 \times 509 \times 259949$
17	$3^2 \times 11 \times 225498914387$
18	$3^2 \times 11 \times 163 \times 20143 \times 1162943$
19	$3^2 \times 11 \times 19727 \times 3471827581$
20	$3^2 \times 11 \times 29 \times 43 \times 1621 \times 641751001$
21	$3^2 \times 11^2 \times 53 \times 67 \times 662348503367$
22	$3^2 \times 11 \times 877 \times 3203 \times 41051 \times 4699727$
23	$3^2 \times 11 \times 11895484822660898387$
24	$3^2 \times 11 \times 139 \times 2129333 \times 922459185301$
25	$3^2 \times 11 \times 37^2 \times 29131483 \times 163992440081$
26	$3^2 \times 11 \times 454823 \times 519472957 \times 690821017$
27	$3^2 \times 11 \times 107 \times 173 \times 7823 \times 12227 \times 1281439 \times 1867343$
28	$3^2 \times 11 \times 431363 \times 2882477797 \times 91865833117$
29	$3^2 \times 11 \times 191 \times 47793258077 \times 349882390108241$
30	$3^2 \times 11 \times 37 \times 283 \times 5087 \times 1736655143086866180331$
31	$3^2 \times 11 \times 2771826449193354891007108898387$
32	$3^2 \times 11 \times 1231547 \times 306730217 \times 227214279676815713$
33	$3^2 \times 11 \times 41 \times 163 \times 224677 \times 278437 \times 6562698554476756561$
34	$3^2 \times 11 \times 109 \times 839 \times 2819 \times 40597679 \times 8642572321688037037$
35	$3^2 \times 11 \times 3072603482270933019578343003268898387$
36	$3^2 \times 11 \times 7523968684626643 \times 14280739323850758510209$
37	$3^2 \times 11 \times 542410073 \times 7125524357434108671946525659019$
38	$3^2 \times 11 \times 379 \times 2677 \times 5685998930867 \times 24769422762368668966567$
39	$3^2 \times 11 \times 127 \times 338944799 \times 126050058872020979628982810240819$
40	$3^2 \times 11 \times 956042657 \times 221187999196843747210838711867563891$
41	$3^2 \times 11 \times 8453033680104197032254976173172281742468898387$
42	$3^2 \times 11 \times 1652359939 \times 276306566079013 \times 758627421394906687355741$

approximately $e^{-1}/6$. Otherwise, if $!p \bmod p > 10$, then

$$(!n \bmod p^2) \bmod p = !p \bmod p > 10 \text{ for } p \leq n \leq 2p,$$

and therefore there cannot be an entry (p, \cdot, \cdot) in Table 3.

TABLE 3. The small values of $!n \bmod p^2 < 10$, for $p \in P$, $p < 2^{20}$, $1 \leq n \leq 2p$

p	n	$!n \bmod p^2$	p	n	$!n \bmod p^2$
2	3	0	83	60	5
2	4	2	163	183	4
3	4	1	163	273	4
3	5	7	173	152	3
3	6	1	197	355	9
5	5	9	373	185	6
5	6	4	373	514	2
5	9	9	467	730	3
7	6	7	467	902	3
11	13	1	3119	306	6
11	21	1	4357	837	7
17	7	7	7717	9402	7
17	11	6	7717	15415	7
19	17	9	8297	4727	7
19	20	9	33703	39795	9
37	25	1	33703	43801	9
37	63	5	33703	52337	9
41	55	4	41611	26144	1
43	9	9	54503	26541	0
47	19	8	302837	283148	8
59	41	9	351731	135646	8
67	29	8			

REFERENCES

1. K. Akiyama, Y. Kida, F. O'Hara, APRT-CLE, Cohen-Lenstra version of Adleman-Pomerance-Rumely Test, UBASIC program, 1988-1992.
2. G. Gogić, *Parallel algorithms in arithmetic*, Master thesis, Belgrade University, 1991.
3. R. Guy, *Unsolved problems in number theory*, Second Edition, Springer-Verlag, 1994. MR **96e**:11002
4. A. Ivić, Ž. Mijajlović, *On Kurepa's problems in number theory*, Publ. Inst. Math. (Beograd) (N. S.), **57(71)**, 1995, 19-28 MR **97a**:11007
5. Y. Kida, ECMX, Prime Factorization by ECM, UBASIC program, 1987-1990.
6. D. E. Knuth, *The Art of Computer Programming*, Vol. 2 Addison-Wesley, Reading 1969. MR **44**:3531
7. Dj. Kurepa, *On the left factorial function*, Math. Balkanica, **1**, 1971, 147-153. MR **44**:3945
8. B. Malešević, Personal communication.
9. Ž. Mijajlović, *On some formulas involving $!n$ and the verification of the $!n$ hypothesis by use of computers*, Publ. Inst. Math. (Beograd), **47(61)**, 1990, 24-32. MR **92d**:11134
10. H. Riesel, *Prime numbers and computer methods for factorization*, Birkhauser, Boston, 1985. MR **88k**:11002
11. UBASIC, version 8.74, 1994.

MATEMATIČKI FAKULTET, BEOGRAD

E-mail address: ezivkovm@matf.bg.ac.yu