PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 100(114) (2016), 101–106 DOI: 10.2298/PIM1614101A

ON DISTINCT RESIDUES OF FACTORIALS

Vladica Andrejić and Miloš Tatarević

ABSTRACT. We investigate the existence of primes $p > 5$ for which the residues of $2!$, $3!$, ..., $(p-1)!$ modulo p are all distinct. We describe the connection between this problem and Kurepa's left factorial function, and report that there are no such primes less than 10^{11}.

1. Introduction

Paul Erdős asked the following question: Is there a prime $p > 5$ such that the residues of $2!, 3!, \dots, (p-1)!$ modulo p are all distinct? Rokowska and Schinzel [**5**] proved that if such p exists, it needs to satisfy the following conditions

$$p \equiv 5 \pmod 8, \quad \left(\frac{5}{p}\right) = -1, \quad \left(\frac{-23}{p}\right) = 1, \tag{1.1}$$

and that the missing residue must be that of $-((p-1)/2)!$. The given conditions enabled them to prove that there are no such primes p with $5 < p < 1000$. This problem is also mentioned in [**2**, Section F11]. Recently, Trudgian [**6**] called such a prime p a socialist prime and proved that p also needs to satisfy

$$\begin{aligned}&\left(\frac{1957}{p}\right) = 1, \text{ or } \left(\frac{1957}{p}\right) = -1 \text{ with } \left(\frac{4y+25}{p}\right) = -1\\ &\qquad\qquad \text{for all } y \text{ satisfying } y(y+4)(y+6) - 1 \equiv 0 \pmod p.\end{aligned} \tag{1.2}$$

He confirmed that there are no such primes less than 10^9.

In this paper, we describe the connection between the socialist primes and the left factorial function $!n = 0! + 1! + \cdots + (n-1)!$ introduced by Đuro Kurepa [**4**]. Kurepa conjectured that $\gcd(!n, n!) = 2$ holds for all integers $n > 1$, which is equivalent to the statement that there is no odd prime p that divides $!p$. This conjecture is also mentioned in [**2**, Section B44].

In our previous work [**1**], we calculated and recorded the residues $r_p = !p \bmod p$ for all primes $p < 2^{34}$. Now we show that if p is a socialist prime then $(!p-2)^2 \equiv -1 \pmod p$, which enabled us to immediately confirm that there are no such primes less than 2^{34}. Additionally, we extended the search up to 10^{11}.

2010 *Mathematics Subject Classification:* Primary 11B83; Secondary 11K31.
Key words and phrases: left factorial, factorial, prime numbers.
Communicated by Žarko Mijajlović.

2. Left factorial calculations

Let us demonstrate some straightforward calculations. Wilson's theorem states that

$$(p-1)! \equiv -1 \pmod{p}, \tag{2.1}$$

for all primes p. Therefore,

$$(p-2)! \equiv 1 \pmod{p}, \tag{2.2}$$

and more generally

$$(p-k)!(k-1)! \equiv (-1)^k \pmod{p}, \tag{2.3}$$

for all primes p and all $1 \leqslant k \leqslant p$. Especially, we have $(((p-1)/2)!)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$. Since in (2.1) and (2.2) we already have residues -1 and 1, if p is a socialist prime, it follows that $((p-1)/2)! \not\equiv \pm 1 \pmod{p}$, so $(-1)^{(p+1)/2} \neq 1$, thus $p \equiv 1 \pmod{4}$, and consequently

$$\Big(\Big(\frac{p-1}{2}\Big)!\Big)^2 \equiv -1 \pmod{p}. \tag{2.4}$$

Let r be the missing residue. Then we have

$$(p-1)! \equiv r \prod_{k=2}^{p-1} k! = r(p-2)!(p-1)!\Big(\frac{p-1}{2}\Big)! \prod_{k=3}^{(p-1)/2} (p-k)!(k-1)! \pmod{p},$$

which after (2.1), (2.2), (2.3), and (2.4) leads to $r \equiv (-1)^{(p^2-1)/8}((p-1)/2)! \pmod{p}$. Since $r \not\equiv ((p-1)/2)! \pmod{p}$, we have

$$r \equiv -\Big(\frac{p-1}{2}\Big)! \pmod{p}. \tag{2.5}$$

Consequently, $(p^2-1)/8$ is odd, and therefore, $p \equiv 5 \pmod{8}$.

Since (2.5), we can connect a socialist prime p with the left factorial function. We have

$$-\Big(\frac{p-1}{2}\Big)! + \sum_{k=2}^{p-1} k! \equiv \sum_{i=1}^{p-1} i = \frac{(p-1)p}{2} \equiv 0 \pmod{p},$$

which implies

$$\Big(\frac{p-1}{2}\Big)! \equiv \sum_{k=2}^{p-1} k! = \sum_{k=0}^{p-1} k! - 2 = !p - 2 \pmod{p}.$$

Finally (2.4) gives the necessary condition

$$(!p-2)^2 \equiv -1 \pmod{p}. \tag{2.6}$$

In our previous work [**1**], we calculated and recorded the residues $r_p = !p \pmod{p}$ for all primes $p < 2^{34}$. After a fast search through our database, the only primes where p divides $(r_p - 2)^2 + 1$ with $p < 2^{34}$ are 5, 13, 157, 317, 5449, and 5749. More concretely, $r_5 = 4$, $r_{13} = 10$, $r_{157} = 131$, $r_{317} = 205$, $r_{5449} = 4816$, and $r_{5749} = 808$. Consequently, there are no socialist primes p with $5 < p < 2^{34}$. It is interesting that there are no small $p \equiv 3 \pmod{4}$ with $p \mid (r_p - 2)^2 + 1$.

In [**1**], we also considered Kurepa's generalized left factorial

$$!^k n = (0!)^k + (1!)^k + \cdots + ((n-1)!)^k,$$

where $!^1 k = !k$. There we presented counterexamples for the analog of Kurepa's conjecture, where for all $1 < k < 100$ there exists an odd prime p such that $p \mid !^k p$. Similarly, we can connect the socialist primes with a generalized left factorial in the following way. From

$$p^{n+1} - 1 = \sum_{m=1}^{p-1} ((m+1)^{n+1} - m^{n+1}) = \sum_{m=1}^{p-1} \sum_{k=0}^{n} \binom{n+1}{k} m^k,$$

we have

$$p^{n+1} - 1 = p - 1 + \sum_{k=1}^{n} \binom{n+1}{k} \sum_{m=1}^{p-1} m^k,$$

and therefore,

$$\sum_{k=1}^{n} \binom{n+1}{k} (1^k + 2^k + \cdots + (p-1)^k) \equiv 0 \pmod{p}$$

for all n, which gives $1^k + 2^k + \cdots + (p-1)^k \equiv 0 \pmod{p}$ for all $1 \leqslant k \leqslant p-2$. Thus

$$(2!)^k + \cdots + ((p-1)!)^k + \Big(-\Big(\frac{p-1}{2}\Big)!\Big)^k \equiv 1^k + 2^k + \cdots + (p-1)^k \equiv 0 \pmod{p}$$

and hence

$$!^k p = (0!)^k + \cdots + ((p-1)!)^k \equiv 2 - \Big(-\Big(\frac{p-1}{2}\Big)!\Big)^k \pmod{p}.$$

If we include (2.4), we finally get the necessary condition:

$$\begin{aligned} (!^k p - 2)^2 + 1 &\equiv 0 \pmod{p} \quad \text{if } k \text{ is odd},\\ !^k p &\equiv 1 \pmod{p} \quad \text{if } k = 4t,\\ !^k p &\equiv 3 \pmod{p} \quad \text{if } k = 4t+2. \end{aligned} \tag{2.7}$$

3. Additional calculations

Let us consider the set $H = \{2, 3, 4, \ldots, p-3\} \setminus \{\frac{p-1}{2}\}$ and let p be a socialist prime. There is a function f defined on H, such that for all $k \in H$,

$$(f(k))! \equiv -k! \pmod{p}. \tag{3.1}$$

Thus, f is an involution on the set H. By using (2.3) after we multiply (3.1) by $(p-1-f(k))!(p-1-k)!$ we get

$$(-1)^{f(k)+1}(p-1-k)! \equiv -(-1)^{k+1}(p-1-f(k))! \pmod{p}. \tag{3.2}$$

Since $(p-1-k)! \not\equiv (p-1-f(k))! \pmod{p}$, we conclude that $f(k) \equiv k \pmod{2}$. This splits the set H into $(p-5)/4$ quadruples with a shape

$$U_k = \{k, f(k), p-1-k, p-1-f(k)\}$$

with $\prod_{x\in U_k} x \equiv 1$, $\sum_{x\in U_k} x \equiv 0 \pmod{p}$, and $x \equiv y \pmod{2}$ for all $x, y \in U_k$.

One idea can be related to $!^k p$ for not fixed k, for example $k = (p-1)/2$. Since

$$\left(\frac{x!}{p}\right) = \left(\frac{-(f(x)!)}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{f(x)!}{p}\right) = \left(\frac{f(x)!}{p}\right), \left(\frac{x!}{p}\right) = \left(\frac{\frac{1}{x!}}{p}\right),$$

we see that all members of U_k have the same quadratic residue modulo p. In this quadruple two members are less than $(p-1)/2$, and therefore,

$$\left(\frac{2!\cdot 3!\cdots \frac{p-3}{2}!}{p}\right) = 1,$$

or more strictly $\left(\frac{2!\cdot 4!\cdots((p-5)/2)!}{p}\right) = 1 = \left(\frac{3!\cdot 5!\cdots((p-3)/2)!}{p}\right)$. Then we have

$$1 = \left(\frac{2!\cdot 3!\cdots \frac{p-3}{2}!}{p}\right) = \left(\frac{3\cdot 5\cdots \frac{p-3}{2}}{p}\right) = \left(\frac{\frac{p-3}{2}!!}{p}\right) = \left(\frac{(\frac{p-1}{2}!)/(2^{\frac{p-1}{4}}\frac{p-1}{4}!)}{p}\right).$$

Since $\left(\frac{((p-1)/2)!}{p}\right) = (((p-1)/2)!)^{(p-1)/2} = (-1)^{(p-1)/4} = -1$ and $\left(\frac{2^{(p-1)/4}}{p}\right) = \left(\frac{2}{p}\right)^{(p-1)/4} = \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = -1$, we can conclude that

$$\left(\frac{\frac{p-1}{4}!}{p}\right) = 1.$$

4. Heuristic considerations

Let us suppose that factorials $2!, 3!, \ldots, (p-1)!$ modulo p are random nonzero integers. The probability that p is a socialist prime can be estimated by

$$1 \times \frac{p-2}{p-1} \times \frac{p-3}{p-1} \times \cdots \times \frac{2}{p-1} = \frac{(p-2)!}{(p-1)^{p-3}}.$$

If we include the fact that $(k+1)! \not\equiv k!$ for $2 \leqslant k \leqslant p-2$, then the estimated probability is slightly higher

$$W_p = 1 \times \frac{p-2}{p-2} \times \frac{p-3}{p-2} \times \cdots \times \frac{2}{p-2} = \frac{(p-2)!}{(p-2)^{p-3}}.$$

From Stirling's approximation, we have $k! \approx \sqrt{2\pi k}\left(\frac{e}{k}\right)^k \leqslant e k^{k+\frac{1}{2}} e^{-k}$, and consequently

$$W_p \leqslant (p-2)^{\frac{3}{2}} e^{3-p}. \tag{4.1}$$

Note that this is just a rough upper bound. If conditions (1.1) and (1.2) are included, this estimation can be reduced by some factor. If we make an assumption that any $!^k p \pmod{p}$ for $k = 1, \ldots, p-2$ is an independent and random number, by including the condition (2.7) one can conclude that $W_p \approx p^{2-p}$. However, we have that $!^{2k} p \equiv\, !^{p-2k-1} p \pmod{p}$ for $1 \leqslant k \leqslant (p-3)/2$ and odd primes p, which implies that W_p should be greater than previously assumed.

Further, we can estimate the number of socialist primes in an interval $[a,b]$ as a sum of W_p over the primes

$$\sum_{a\leqslant p\leqslant b} W_p \approx \sum_{n=a}^{b} W_{n\ln n} \approx \int_a^b W_{t\ln t}\,dt.$$

From (4.1), we can see that $W_p < e^3 p^{\frac{3}{2}} e^{-p}$, therefore,

$$\begin{aligned}\sum_{a\leqslant p\leqslant b} W_p &< e^3 \int_a^b t^{\frac{3}{2}-t}(\ln t)^{\frac{3}{2}}\,dt \\ &< e^3 \int_a^b t^{\frac{3}{2}-t}(\ln t)^{\frac{3}{2}}\Big(1+\frac{1}{\ln t}-\frac{3}{2t\ln t}-\frac{1}{2t(\ln t)^2}\Big)dt \\ &< e^3 \int_a^b \Big(-t^{\frac{3}{2}-t}(\ln t)^{\frac{1}{2}}\Big)'\,dt\end{aligned}$$

and thus

$$\sum_{a\leqslant p\leqslant b} W_p < e^3 a^{\frac{3}{2}-a}\sqrt{\ln a}.$$

According to the last statement, we expect no more than $e^3 a^{\frac{3}{2}-a}\sqrt{\ln a}$ socialist primes greater than a. As we confirmed that there are no socialist primes less than 10^{11}, the estimated probability that such primes exist is less than $10^{-10^{12}}$.

5. Computer search

In 1960, Rokowska and Schinzel [**5**] reported that there are no primes p with $5 < p < 1000$ for which the residues of $2!, 3!, \ldots, (p-1)!$ modulo p are all distinct. By applying the conditions (1.1), there are only ten primes below 1000 that need to be examined. For $5 < p < 10^6$, there are only 4908 such primes, and after applying (1.2) this is further reduced to 3662 primes [**6**]. Recently, Trudgian [**6**] confirmed that there are no such primes less than 10^9.

As a part of the search for a counterexample to Kurepa's conjecture, we recorded the residues $r_p = {!p} \bmod p$ for all $p < 2^{34}$ [**1**]. By using the congruence (2.6), we instantly verified that there are no such primes p that satisfy this condition for $10^9 < p < 2^{34}$. To extend the range beyond 2^{34} we need a more efficient method, as the time complexity of the algorithm to obtain r_p for all $p < n$ is $O(n^2/\ln n)$.

To show that p is not a socialist prime, it is sufficient to find a single pair of integers i and j, such that $2 \leqslant i < j \leqslant p-1$ and $i! \equiv j! \pmod p$. As we can consider that $i!$ and $j!$ modulo p are "random" integers, to find such a pair we can apply a well-known probabilistic method called the birthday attack. On average, it is expected that first such a pair will be found after approximately $\sqrt{p\pi/2}$ attempts [**3**]. The time complexity of this algorithm is $O(\sqrt{p})$ for single p, and $O(n^{3/2}/\ln(n))$ for all $p < n$. As we already mentioned, we do not need to examine all the primes. To simplify the calculation, we used congruences given in (1.1). Note that in this case, the time complexity remains the same as the search space is reduced by the constant factor. Using this method, we confirmed that there are no socialist primes less than 10^{11}.

For our computation, we used a single Intel Core i7-4980HQ CPU running at 2.8GHz. This CPU natively supports 64-bit multiplication without overflow, which allows us to implement a rapid modular reduction. Note that we do not necessarily need to search for the first occurrence of two the same factorials modulo p. In our implementation, we made several changes that, on average, slightly increased the number of iterations required to register these duplicates, but overall they made the execution faster.

To reduce the memory consumption, we used an array of integers as a simple hash table without collision resolution. Accessing the elements of the hash table can be slow if accessed memory blocks are not in the cache. The CPU we used has 256KB of L2 cache per core and 6MB of shared L3 cache. While we focus on primes less than 10^{11}, we can rarely expect more than $4 \cdot 10^5$ iterations before the first duplicate is discovered. This number of iterations is large enough to assume that it will be hard to keep all the data in the L2 cache. Using the right size of the array we targeted the efficient usage of L3 cache. Various sizes of arrays were tested, and the best parameters were determined empirically. In particular, for p in the region of 10^{11}, an array of 2^{19} elements provided good results.

The search for all $p < 10^{11}$ took slightly over one day. Although the search can be extended beyond this bound, it is reasonable to believe that there are no socialist primes, as we explained in Section 4.

Acknowledgement. Partially supported by the Serbian Ministry of Education and Science, project 174012.

References

1. V. Andrejić, M. Tatarević, *Searching for a counterexample to Kurepa's conjecture*, Math. Comput., **85** (2016), 3061–3068.
2. R. Guy, *Unsolved Problems in Number Theory*, 3^{rd} edition, Springer-Verlag, 2004.
3. M. S. Klamkin, D. J. Newman, *Extensions of the birthday surprise*, J. Comb. Theory **3** (1967), 279–282
4. Ð. Kurepa, *On the left factorial function* $!n$, Math. Balk. **1** (1971), 147–153.
5. B. Rokowska, A. Schinzel, *Sur une problème de M. Erdős*, Elem. Math. **15** (1960), 84–85.
6. T. Trudgian, *There are no socialist primes less than* 10^9, Integers **14** (2014), A63.

(Received 19 01 2016)
(Revised 14 03 2016)

Faculty of Mathematics
University of Belgrade
Belgrade
Serbia
andrew@matf.bg.ac.rs

Alameda, CA 94501
USA
milos.tatarevic@gmail.com