Exponential Sums and Congruences with Factorials

Moubariz Z. Garaev
Instituto de Matemáticas, Universidad Nacional Autónoma de México
C.P. 58180, Morelia, Michoacán, México
garaev@matmor.unam.mx

Florian Luca
Instituto de Matemáticas, Universidad Nacional Autónoma de México
C.P. 58180, Morelia, Michoacán, México
fluca@matmor.unam.mx

Igor E. Shparlinski
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

August 14, 2018

Abstract

We estimate the number of solutions of certain diagonal congruences involving factorials. We use these results to bound exponential sums with products of two factorials $n!m!$ and also derive asymptotic formulas for the number of solutions of various congruences with factorials. For example, we prove that the products of two factorials $n!m!$ with $\max\{n, m\} < p^{1/2+\varepsilon}$ are uniformly distributed modulo $p$, and that any residue class modulo $p$ is representable in the form $m!n! + n_1! + \ldots + n_{49}!$ with $\max\{m, n, n_1, \ldots, n_{49}\} < p^{8775/8794+\varepsilon}$.

2000 Mathematics Subject Classification: 11A07, 11B65, 11L40.
1 Introduction

Throughout this paper, $p$ is an odd prime. Very little seems to be known, or even conjectured, about the distribution of $n!$ modulo $p$. In F11 in [3], it is conjectured that about $p/e$ of the residue classes $a \pmod{p}$ are missed by the sequence $n!$. If this were so, the sequence $n!$ modulo $p$ should assume about $(1 - 1/e)p$ distinct values. Some results of this spirit have appeared in [3].

The scarcity of heuristic results is probably due to the hardness of computing factorials. The best known algorithm to compute $n!$ over $\mathbb{Z}$ or modulo $p$ takes about $n^{1/2}$ arithmetic operations in the corresponding ring, see [1, 2]. It has been shown in [21] that the complexity of computing factorials is related to such deep conjectures of the complexity theory as the algebraic version of the $P = NP$ question, see also a nice discussion in [2].

Sums of multiplicative characters and various additive and multiplicative congruences with factorials have been considered in [6, 7, 19]. In particular, it is has been shown in [7] that for any nonprincipal character $\chi$ modulo $p$ we have

$$
\sum_{n=L+1}^{L+N} \chi(n!) = O \left( N^{3/4}p^{1/8}(\log p)^{1/4} \right)
$$

and also that the number of solutions $I_\ell(L, N)$ of the congruence

$$
n_1! \ldots n_\ell! \equiv n_{\ell+1}! \ldots n_{2\ell}! \pmod{p}, \quad L < n_1, \ldots, n_{2\ell} \leq L + N,
$$

satisfies the bound

$$
I_\ell(L, N) \ll N^{2\ell-1+2^\ell-1}
$$

(provided $0 \leq L < L + N < p$).

Using (1) and (2), it has been shown in [4] that for any fixed $\varepsilon > 0$ the products of three factorials $n_1!n_2!n_3!$, with $\max\{n_1, n_2, n_3\} = O(p^{5/6+\varepsilon})$ are uniformly distributed modulo $p$. Here, we obtain an upper bound for the additive analogue of (2) and use it to estimate double exponential sums with products of two factorials. Namely, for integers $a, K, L, M$ and $N$ we consider double exponential sums

$$
W_a(K, M; L, N) = \sum_{m=K+1}^{K+M} \sum_{n=L+1}^{L+N} e(am!n!),
$$
where we define
\[ e(z) = \exp(2\pi iz/p). \]

In turn, our bound of exponential sums \( W_a(K, M; L, N) \) lead us to a substantial improvement of the aforementioned result, showing that the products of two factorials \( n!m! \), with \( \max\{n, m\} = O(p^{1/2+\varepsilon}) \), are uniformly distributed modulo \( p \). We then combine our new bounds and the bounds (1) and (3) to study various congruences involving factorials.

Studying single exponential sums
\[ S_a(L, N) = \sum_{n=L+1}^{L+N} e(an!) \]
is of great interest too. Although we have not been able to obtain “individual” bounds for these sums, we obtain various bounds “on average”, which also play a crucial role in our arguments.

Some results and techniques of [7] have found their applications to studying prime divisors of \( n! + f(n) \) for various functions \( f \), see [17] [18]. In particular, in [17] they have led to an improvement of a result of Erdős and Stewart [5]. We expect that the results of this work will also find some applications to various arithmetic questions.

Throughout the paper, the implied constants in symbols ‘\( O \)’ and ‘\( \ll \)’ may occasionally, where obvious, depend on integer parameters \( k, \ell, r \) and a small real parameter \( \varepsilon > 0 \), and are absolute otherwise (we recall that \( U \ll V \) and \( A = O(B) \) are both equivalent to the inequality \( |U| \leq cV \) with some constant \( c > 0 \)).

Acknowledgements. During the preparation of this paper, F. L. was supported in part by grants SEP-CONACYT 37259-E and 37260-E, and I. S. was supported in part by ARC grant DP0211459.
2 Bounds on the Number of Solutions of Additive Congruences with Factorials

For integers $\ell \geq 1$, $\lambda$, $L$ and $N$ with $0 \leq L < L + N < p$ we denote by $J_\ell(L, N; \lambda)$ the number of solutions to the congruence

$$\sum_{i=1}^\ell n_i! \equiv \sum_{i=\ell+1}^{2\ell} n_i! + \lambda \pmod{p}, \quad L + 1 \leq n_1, \ldots, n_{2\ell} \leq L + N.$$  

We also put $J_\ell(L, N) = J_\ell(L, N, 0)$.

Our treatment of $J_\ell(L, N; \lambda)$ is based on exponential sums. Accordingly, we recall the identity

$$\sum_{a=0}^{p-1} e(au) = \begin{cases} 0, & \text{if } u \not\equiv 0 \pmod{p}, \\ p, & \text{if } u \equiv 0 \pmod{p}, \end{cases}$$

which we will repeatedly use, in particular to relate the number of solutions of various congruences and exponential sums.

**Theorem 1.** Let $L$ and $N$ be integers with $0 \leq L < L + N < p$. Then for any positive integer $\ell \geq 1$, the inequality

$$J_\ell(L, N; \lambda) \ll N^{2\ell-1+1/(\ell+1)}$$

holds.

**Proof.** The identity (4) implies that

$$J_\ell(L, N; \lambda) = \frac{1}{p} \sum_{a=0}^{p-1} |S_a(L, N)|^{2\ell} e(-a\lambda). \quad (5)$$

In particular

$$J_\ell(L, N; \lambda) \leq J_\ell(L, N) = \frac{1}{p} \sum_{a=0}^{p-1} |S_a(L, N)|^{2\ell}.$$

For any integer $k \geq 0$ we have

$$S_a(L, N) = \sum_{n=L+1}^{L+N} e(a(n+k)! + O(k)).$$
Therefore, for any integer $K \geq 0$,

$$S_a(L, N) = \frac{1}{K} \sum_{k=0}^{K-1} \sum_{n=L+1}^{L+N} e(a(n+k)! + O(K))$$

$$= \frac{1}{K} \sum_{n=L+1}^{L+N} \sum_{k=1}^{K} e \left( a n! \prod_{i=1}^{k} (n+i) \right) + O(K)$$

$$= \frac{1}{K} \sum_{n=L+1}^{L+N} \sum_{k=0}^{K-1} e \left( a n! \prod_{i=1}^{k} (n+i) \right) + O(K).$$

Using the Hölder inequality, we derive

$$\sum_{a=0}^{p-1} |S_a(L, N)|^{2\ell} \ll K^{-2\ell} N^{2\ell-1} \sum_{k_1, \ldots, k_{2\ell}=0}^{K-1} \sum_{n=L+1}^{L+N} \sum_{a=0}^{p-1} e \left( a n! \Phi_{k_1, \ldots, k_{2\ell}}(n) \right) + p K^{2\ell},$$

where

$$\Phi_{k_1, \ldots, k_{2\ell}}(X) = \sum_{\nu=1}^{\ell} \prod_{i=1}^{k_\nu} (n+i) - \sum_{\nu=\ell+1}^{2\ell} \prod_{i=1}^{k_\nu} (n+i).$$

The sum over $a$ vanishes, unless

$$n! \Phi_{k_1, \ldots, k_{2\ell}}(n) \equiv 0 \pmod{p}, \quad (6)$$

in which case it equals $p$.

It is easy to see that $\Phi_{k_1, \ldots, k_{2\ell}}(X)$ is a nonconstant polynomial of degree $O(K)$, unless $(k_1, \ldots, k_{2\ell})$ is a permutation of $(k_{\ell+1}, \ldots, k_{2\ell})$, which happens for $O(K^{2\ell})$ choices of $0 \leq k_1, \ldots, k_{2\ell} \leq K-1$. If $\Phi_{k_1, \ldots, k_{2\ell}}(X)$ is a nonconstant polynomial, then (6) is satisfied for at most $K$ values of $n$, otherwise we use the trivial bound $N$ on the number of solutions in $n$.

Because $n! \not\equiv 0 \pmod{p}$ for $0 \leq L < n \leq L+N < p$, the total number of solutions of (6) in $L+1 \leq n \leq L+N$ and $0 \leq k_1, \ldots, k_{2\ell} \leq K-1$ is $O(NK^{\ell} + K^{2\ell+1})$.

Thus

$$\sum_{a=0}^{p-1} |S_a(L, N)|^{2\ell} \ll K^{-2\ell} N^{2\ell-1} (NK^{\ell} + K^{2\ell+1}) p + K^{2\ell} p$$

$$= \left(N^{2\ell} K^{-\ell} + N^{2\ell-1} K + K^{2\ell}\right) p.$$

Taking $K = \lceil N^{1/(\ell+1)} \rceil$ and remarking that with this value of $K$ the last term never dominates, we finish the proof. \qed
Corollary 2. Let $\delta_i = \pm 1$ for each $i = 1, \ldots, k$. Then for any integer $\lambda$, the number of solutions of the congruence
\[
\sum_{i=1}^{k} \delta_i n_i! \equiv \lambda \pmod{p}, \quad L + 1 \leq n_1, \ldots, n_k \leq L + N,
\]
is $O \left( N^{k-1+1/(k_1+1)+1/(k_2+1)} \right)$, where $k_1 = \lfloor k/2 \rfloor$, $k_2 = \lfloor (k + 1)/2 \rfloor$.

Proof. Note that $k = k_1 + k_2$. By the identity (4), the number $J$ of solutions of the above congruence can be expressed via exponential sums as
\[
J = \frac{1}{p} \sum_{n_1, \ldots, n_k = L+1}^{L+N} \sum_{a=0}^{p-1} e \left( a \left( \sum_{i=1}^{k} \delta_i n_i! - \lambda \right) \right)
= \frac{1}{p} \sum_{a=0}^{p-1} e(-a\lambda) \prod_{i=1}^{k} S_{\delta_i}(L, N).
\]
Since $|S_{\delta_i}(L, N)| = |S_{\lambda}(L, N)|$, we see that
\[
J \leq \frac{1}{p} \sum_{a=0}^{p-1} |S_{\lambda}(L, N)|^k = \frac{1}{p} \sum_{b=0}^{p-1} |S_{\lambda}(L, N)|^{k_1} |S_{\lambda}(L, N)|^{k_2}.
\]
Using the Cauchy inequality and Theorem 1 (see also (3)), we finish the proof. \qed

Let $F_\ell(K, M; L, N)$ denote the number of solutions of the congruence
\[
\sum_{i=1}^{\ell} n_i!m_i! \equiv \sum_{i=\ell+1}^{2\ell} n_i!m_i! \pmod{p},
\]
$K + 1 \leq m_1, \ldots, m_{2\ell} \leq K + M$, $L + 1 \leq n_1, \ldots, n_{2\ell} \leq L + N$.

The condition $N^2 \geq M \geq N^{1/2}$, requested in our next result can be substantially relaxed. However, because we are mainly interested in the “diagonal case” $M = N$ (for which this condition is always satisfied) and in order to avoid some technical complications, we use this condition.

Theorem 3. Let $K$, $L$, $M$ and $N$ be integers with $0 \leq K < K + M < p$ and $0 \leq L < L + N < p$. For any positive integer $\ell \geq 1$, such that $N^2 \geq M \geq N^{1/2}$, the following bound holds
\[
F_\ell(K, M; L, N) \ll M^{2\ell-1+1/2\ell} N^{2\ell-1/2(\ell+1)}.
\]
Proof. First of all we note that if we prove the above inequality for $N^2 \geq M \geq N$ then we are done. Indeed, if $N > M \geq N^{1/2}$ then we have $M^2 \geq N \geq M$, and the statement follows from the inequality
\[
N^{2\ell-1+1/2\ell} M^{2\ell-1/2(\ell+1)} \ll M^{2\ell-1+1/2\ell} N^{2\ell-1/2(\ell+1)}.
\]

So, let $N^2 \geq M \geq N$. We set $H = \lceil M^{1/2\ell} N^{1/2(\ell+1)} \rceil$. We see that $N^{1/2(\ell+1)} \ll H \ll M^{1/2(\ell+1)}$. Then, by the identity (4),
\[
F_\ell(K, M; L, N) = \frac{1}{p^{\ell}} \sum_{a=0}^{p-1} \left| \sum_{m=K+1}^{K+M} \sum_{n=L+1}^{L+N} e(amn!) \right|^{2\ell}
\]
\[
= \frac{1}{p^{\ell}} \sum_{a=0}^{p-1} \left| \sum_{r=1}^{H} \sum_{K+(r-1)M/H < m \leq K+rM/H}^{K+M} \sum_{n=L+1}^{L+N} e(amn!) \right|^{2\ell}.
\]

Applying the Hölder inequality, we obtain
\[
F_\ell(K, M; L, N) \ll H^{2\ell-1} Q,
\]
where $Q$ is the number of solutions of the congruence (7) with the additional condition that $|m_i - m_j| \leq M/H$, $1 \leq i < j \leq 2\ell$. Without loss of generality, we may suppose that $m_1 = \min\{m_i \mid 1 \leq i \leq 2\ell\}$. We denote $m_1 = m$ and put
\[
m_i = m + s_i, \quad 2 \leq i \leq 2\ell.
\]

Then the congruence (7) in the new variables takes the form
\[
n_1! + \sum_{i=2}^{\ell} f(m, s_i)n_i! - \sum_{i=\ell+1}^{2\ell} f(m, s_i)n_i! \equiv 0 \pmod{p}, \quad (8)
\]
where $f(m, t) = (m + 1) \ldots (m + t)$ for an integer $t \geq 1$ and $f(n, 0) = 1$.

The number of solutions of the congruence (8) is collected from two sets of variables $m$ and $n_i, s_i$, $1 \leq i \leq 2\ell$: 7
(i) the first set is such that the left hand side of (8) is a polynomial of $m$
of degree greater than zero (but less than $M/H$);

(ii) the second set consists of those for which the left hand side of (8) isconstant as a polynomial of $m$.

The number of solutions $Q_1$ of (8) corresponding to the first set is at most

$$Q_1 \leq N^{2\ell} \left( \frac{M}{H} + 1 \right)^{2\ell-1} \frac{M}{H} \ll (MN/H)^{2\ell}.$$ 

For the second set of variables, we have that as a polynomial, the left hand side of (8) is a constant. Let us numerate $s_2, \ldots, s_{2\ell}$ in an increasing order. Then, instead of equation (8) we consider the equation

$$n_1! + \delta_i \sum_{i=2}^{2\ell} f(m, r_i) n_i! \equiv 0 \pmod{p},$$

with $\delta_i = \pm 1$, and such that

$$0 = r_1 \leq \ldots \leq r_{2\ell} \leq M/H.$$ 

Moreover, for each positive integer $k \leq 2\ell$ and positive integers $e_1, \ldots, e_k$, we consider solutions with

$$0 = r_1 = \ldots = r_{e_1} < r_{e_1+1} = \ldots = r_{e_1+e_2} < \ldots$$

$$< r_{e_1+\ldots+e_{k-1}+1} = \ldots = r_{e_1+\ldots+e_k} \leq M/H. \quad (9)$$

In this case, the vanishing of the polynomial in $m$ on the left hand side of (8) leads to the conditions

$$n_1! + \delta_2 n_2! + \ldots + \delta_{e_1} n_{e_1}! \equiv 0 \pmod{p},$$

$$\delta_{e_1+1} n_{e_1+1}! + \ldots + \delta_{e_1+e_2} n_{e_1+e_2}! \equiv 0 \pmod{p},$$

$$\ldots$$

$$\delta_{e_1+\ldots+e_{k-1}+1} n_{e_1+\ldots+e_{k-1}+1}! + \ldots + \delta_{e_1+\ldots+e_k} n_{e_1+\ldots+e_k}! \equiv 0 \pmod{p}. \quad (10)$$

Certainly, for each solution to the system of congruences (10) there are at most $M$ possible values for $m$. We also note that from (10) it follows that $e_i \geq 2$ for $1 \leq i \leq k$. In particular, $k \leq \ell$.  

8
For each $k$-dimensional vector $\mathbf{e} = (e_1, \ldots, e_k)$ of positive integers such that $e_1 + \ldots + e_k = 2\ell$, there are $O\left((M/H)^{k-1}\right)$ possible integer vectors $(r_1, \ldots, r_{2\ell})$ satisfying (9). For each such fixed vector $(r_1, \ldots, r_{2\ell})$, the number of solutions of the system of congruences (10), by Corollary 2, is at most

$$O\left(\prod_{\nu=1}^{k} N^{r_{\nu}-1+1/2([e_i/2]+1)+1/2([e_i+1]/2)+1}\right) = O\left(N^{2\ell-k+\kappa(\mathbf{e})}\right),$$

where

$$\kappa(\mathbf{e}) = \sum_{i=1}^{k} \left(\frac{1}{2([e_i/2]+1)} + \frac{1}{2([e_i+1]/2)+1}\right).$$

Therefore,

$$Q_2 \ll \max_{\mathbf{e}} (M/H)^{k-1} MN^{2\ell-k+\kappa(\mathbf{e})},$$

where the maximum is taken over all integers $1 \leq k \leq \ell$ and $k$-dimensional vectors $\mathbf{e} = (e_1, \ldots, e_k)$ of integers $e_i \geq 2, 1 \leq i \leq k$, with $e_1 + \ldots + e_k = 2\ell$.

If $\ell = 1$ then $k = 1$, $\kappa(\mathbf{e}) = 1/2$ and

$$Q_2 \ll MN^{3/2}.$$

Therefore, in this case we have

$$F_\ell(K, M; L, N) \ll M^2 N^2 H^{-1} + MN^{3/2} H,$$

and the required estimate follows from the choice of $H$.

Now, we suppose that $\ell \geq 2$. If $k = 1$, then

$$\kappa(\mathbf{e}) = \frac{1}{\ell+1}.$$

If $k \geq 2$, then trivially

$$\kappa(\mathbf{e}) \leq \frac{k}{2}.$$

Hence,

$$Q_2 \ll MN^{2\ell-\ell/(\ell+1)} + N^{2\ell} H \max_{2 \leq k \leq 2\ell} (M/H N^{1/2})^k.$$

One verifies that for our choice of $H$ and under the condition $N^{\ell+1-1/(\ell+1)} \geq M$ (which is always satisfied for $\ell \geq 2$ and $N^2 \geq M$), we have $M/H N^{1/2} \leq 1$, so the term corresponding to $k = 2$ dominates. Therefore,

$$Q_2 \ll MN^{2\ell-\ell/(\ell+1)} + M^2 N^{2\ell-1} H^{-1}.$$
Thus, putting everything together we obtain,

\[
F_{\ell}(K, M; L, N) \leq H^{2\ell - 1} \left( (MN/H)^{2\ell} + MN^{2\ell - \ell/(\ell + 1)} + M^2 N^{2\ell - 1} H^{-1} \right).
\]

Since \( \ell \geq 2 \) then \( M \leq N^{3\ell/(\ell + 1)} \) for \( N^2 \geq M \). Therefore the first term always dominates the third one, and we derive

\[
F_{\ell}(K, M; L, N) \ll M^{2\ell} N^{2\ell} H^{-1} + MN^{2\ell - \ell/(\ell + 1)} H^{2\ell - 1}.
\]

Recalling our choice of \( H \), we finish the proof. \( \square \)

3 Bounds of Double Exponential Sums with Factorials

Unfortunately we are not able to estimate single sums \( S_a(L, N) \), however we obtain nontrivial bounds for double exponential sums with factorials. We follow some ideas of Karatsuba \([10, 11]\) and Korobov \([13, 14]\), see also Lemma 4 in \([12]\) and the follow-up discussion.

**Theorem 4.** Let \( K, L, M \) and \( N \) be integers with \( 0 \leq K < K + M < p \) and \( 0 \leq L < L + N < p \). Then for any integers \( k, \ell \geq 1 \), the inequality

\[
\max_{\gcd(a,p)=1} |W_a(K, M; L, N)| \ll M^{1-1/2(k+1)} N^{1-1/2k(\ell + 1)} p^{1/2k\ell}
\]

holds.

**Proof.** Let \( G_{\ell}(L, N; \lambda) \) denote the number of solutions to the congruence

\[
\sum_{i=1}^\ell n_i! \equiv \lambda \pmod{p}, \quad L + 1 \leq n_1, \ldots, n_\ell \leq L + N.
\]

Clearly,

\[
\sum_{\lambda=0}^{p-1} G_{\ell}(L, N; \lambda) = N^\ell \quad \text{and} \quad \sum_{\lambda=0}^{p-1} G_{\ell}(L, N; \lambda)^2 = J_{\ell}(L, N). \quad (11)
\]
By the Hölder inequality, we have

\[
|W_a(K, M; L, N)|^\ell \leq M^{\ell - 1} \sum_{m=K+1}^{K+M} \left| \sum_{n=L+1}^{L+N} e(am!n!) \right|^{\ell}
\]

\[
= M^{\ell - 1} \sum_{m=K+1}^{K+M} \left| \sum_{n_{1}, \ldots, n_{2\ell} = L+1}^{L+N} e(am!(n_{1} + \ldots + n_{\ell})) \right|
\]

\[
= M^{\ell - 1} \vartheta_m \sum_{m=K+1}^{K+M} \left| \sum_{n_{1}, \ldots, n_{2\ell} = L+1}^{L+N} e(am!(n_{1} + \ldots + n_{\ell})) \right|
\]

for some complex numbers \( \vartheta_m \) with \( |\vartheta_m| = 1, \) \( K+1 \leq m \leq K+M. \)
Therefore,

\[
|W_a(K, M; L, N)|^\ell = M^{\ell - 1} \sum_{m=K+1}^{K+M} \sum_{\lambda=0}^{p-1} G_{\ell}(L, N; \lambda) \vartheta_m e(a\lambda m!).
\]

Applying the Hölder inequality again, we derive

\[
|W_a(K, M; L, N)|^{2\ell} \leq M^{2\ell(\ell - 1)} \left| \sum_{\lambda=0}^{p-1} G_{\ell}(L, N; \lambda) \sum_{m=K+1}^{K+M} \vartheta_m e(a\lambda m!) \right|^{2\ell}
\]

\[
\leq M^{2\ell(\ell - 1)} \left( \sum_{\lambda=0}^{p-1} G_{\ell}(L, N; \lambda)^{2\ell/(2\ell - 1)} \right)^{2\ell - 1} \sum_{m=K+1}^{K+M} \left| \sum_{\lambda=0}^{p-1} \vartheta_m e(a\lambda m!) \right|^{2\ell - 1}
\]

Once again, by the Hölder inequality,

\[
\left( \sum_{\lambda=0}^{p-1} G_{\ell}(L, N; \lambda)^{2\ell/(2\ell - 1)} \right)^{2\ell - 1} \leq \left( \sum_{\lambda=0}^{p-1} G_{\ell}(L, N; \lambda) \right)^{2\ell - 2} \sum_{\lambda=0}^{p-1} G_{\ell}(L, N; \lambda)^{2}.
\]

Using \([11]\), we obtain

\[
\left( \sum_{\lambda=0}^{p-1} G_{\ell}(L, N; \lambda)^{2\ell/(2\ell - 1)} \right)^{2\ell - 1} \leq N^{2\ell(\ell - 1)} J_{\ell}(L, N).
\]
We now have
\[
\begin{aligned}
    p-1 \sum_{\lambda=0}^{K+M} \left| \sum_{m=K+1}^{K+M} \vartheta_m e(a\lambda m!) \right|^{2k} \\
    = \sum_{\lambda=0}^{p-1} \sum_{m_{1},\ldots,m_{2k}=K+1}^{K+M} \prod_{\nu=1}^{k} \vartheta_{m_{\nu}} e(a\lambda m_{\nu}!) \prod_{\nu=k+1}^{2k} \vartheta_{m_{\nu}} e(-a\lambda m_{\nu}!) \\
    = \sum_{m_{1},\ldots,m_{2k}=K+1}^{K+M} \prod_{\nu=1}^{k} \vartheta_{m_{\nu}} \prod_{\nu=k+1}^{2k} \vartheta_{m_{\nu}} \sum_{\lambda=0}^{p-1} \left( a\lambda \left( \sum_{\nu=1}^{k} m_{\nu}! - \sum_{\nu=k+1}^{2k} m_{\nu}! \right) \right) \\
    \leq pJ_k(K, M).
\end{aligned}
\]

Using Theorem 1, we obtain
\[
|W_a(K, M; L, N)|^{2k\ell} \leq pM^{2k(\ell-1)}N^{2k(k-1)}J_{\ell}(L, N)J_k(K, M) \\
\ll p(MN)^{2k\ell}N^{-\ell/(\ell+1)}M^{-k/(k+1)},
\]
and the desired bound follows. \( \square \)

For example, for every fixed \( \varepsilon > 0 \), choosing sufficiently large \( k \) and \( \ell \), Theorem 4 yields a nontrivial bound whenever \( NM \geq p^{1+\varepsilon} \).

For \( K = L = 0, N = M = p-1 \), choosing \( k = \ell = 2 \), we obtain that the bound of Theorem 4 is of the form \( O(p^{2-1/24}) \).

It is immediate that Theorem 4 combined with the Erdős-Turán relation between the discrepancy and the appropriate exponential sums (see [4, 15]) gives essentially the same the bound (with only an extra factor \( \log p \)) on the discrepancy of the sequence of fractional parts
\[
\left\{ \frac{m!n!}{p} \right\}, \quad K + 1 \leq m \leq K + M, \quad L + 1 \leq n \leq L + N.
\]

As we have remarked, this improves in several directions a similar result from [7].

We also remark that Theorem 3 can be reformulated as an upper bound on the average value of sums \( W_a(K, M; L, N) \) over \( a = 0, \ldots, p-1 \).
4 Asymptotic Formulas for the Number of Solutions of Mixed Congruences with Factorials

Let $T_r(K, M; L, N; \lambda)$ denote the number of solutions of the congruence

$$
\sum_{i=1}^{r} n_i!m_i! \equiv \lambda \pmod{p},
$$

$$
K + 1 \leq m_1, \ldots, m_r \leq K + M, \quad L + 1 \leq n_1, \ldots, n_r \leq L + N.
$$

**Theorem 5.** Let $K$, $L$, $M$ and $N$ be integers with $0 \leq K < K + M < p$ and $0 \leq L < L + N < p$. For any positive integers $k$, $\ell$, $r$ and $s$ such that $s \leq r/2$ and $N^2 \geq M \geq N^{1/2}$, we have

$$
\left| T_r(K, M; L, N; \lambda) - \frac{(MN)^r}{p} \right| \ll M^{r-1+1/2s-(r-2s)/2k(k+1)} N^{r-1/2(s+1)-(r-2s)/2k(\ell+1)} p^{(r-2s)/2k\ell}.
$$

**Proof.** Using the standard principle, we express $T_r(K, M; L, N; \lambda)$ via exponential sums. Then

$$
T_r(K, M; L, N; \lambda) = \frac{1}{p} \sum_{a=0}^{p-1} (W_a(K, M; L, N))^r e(-a\lambda).
$$

Separating the term $(MN)^r/p$ corresponding to $a = 0$, we obtain

$$
\left| T_r(K, M; L, N; \lambda) - \frac{(MN)^r}{p} \right| \leq \frac{1}{p} \sum_{a=0}^{p-1} |W_a(K, M; L, N)|^r
$$

$$
\ll \max_{1 \leq a \leq p-1} |W_a(K, M; L, N)|^{r-2s} \frac{1}{p} \sum_{a=0}^{p-1} |W_a(K, M; L, N)|^{2s}
$$

$$
\leq F_s(K, M; L, N) \max_{1 \leq a \leq p-1} |W_a(K, M; L, N)|^{r-2s}.
$$

Using Theorem 3 and Theorem 4 we finish the proof. $\square$

Taking $M = N$, $r = 7$, $s = 2$, $k = \ell = 2$ in Theorem 4 we derive that any residue class $\lambda$ modulo $p$ has $N^{14} p^{-1} \left( +O(N^{-17/12} p^{11/8}) \right)$ representations in a form

$$
m_1!n_1! + m_2!n_2! + \ldots + m_7!n_7! \equiv \lambda \pmod{p},
$$
with $K + 1 \leq m_1, n_1, \ldots, m_7, n_7 \leq K + N$ (provided $0 \leq K < K + N < p$).

In particular, each $\lambda$ is represented in the above form for $K = 0$ and some $N$ of the size $N = O\left(p^{33/34}\right)$.

For integers $r \geq 0$, $\lambda$, $L$, and $N$ with $0 \leq L < L + N < p$ we denote by $Q_r(K, M; L, N; \lambda)$ the number of solutions of the congruence

$$m!n! + \sum_{1 \leq i \leq r} n_i! \equiv \lambda \pmod{p},$$

with $K + 1 \leq m \leq K + M$ and $L + 1 \leq n, n_1, \ldots, n_{2\ell} \leq L + N$.

**Theorem 6.** Let $K$, $L$, $M$ and $N$ be integers with $0 \leq K < K + M < p$ and $0 \leq L < L + N < p$. Then for any integers $k, \ell \geq 1$, the inequality

$$\left| Q_r(K, M; L, N; \lambda) - \frac{MN^{r+1}}{p} \right| \ll M^{1-1/2(r+1)}N^{r+1/2(r_1+1)+1/2(r_2+1)-1/2(k+1)}p^{1/2kl}$$

holds, where $r_1 = \lfloor r/2 \rfloor$, $r_2 = \lfloor (r + 1)/2 \rfloor$.

**Proof.** We express $Q_r(K, M; L, N; \lambda)$ via exponential sums:

$$Q_r(K, M; L, N; \lambda) = \frac{1}{p} \sum_{a=0}^{p-1} W_a(K, M; L, N) \left(S_a(L, N)\right)^r e(-a\lambda).$$

Selecting the main term $MN^{r+1}/p$, corresponding to $a = 0$, we obtain

$$\left| Q_r(K, M; L, N; \lambda) - \frac{MN^{r+1}}{p} \right| \ll \max_{1 \leq a \leq p-1} |W_a(K, M; L, N)| \frac{1}{p} \sum_{a=0}^{p-1} |S_a(L, N)|^r.$$

Using Theorem 4 and the same arguments as in the proof of Corollary 2 we conclude the proof. \hfill $\square$

Taking $M = N$, $r = 49$, $k = \ell = 2$ in Theorem 6 we derive that any residue class $\lambda$ modulo $p$ has $N^{51}p^{-1} \left(1 + O(N^{-4397/3900}p^{9/8})\right)$ representations in the form

$$m!n! + n_1! + \ldots + n_{49}! \equiv \lambda \pmod{p},$$

14
with $K+1 \leq m, n, n_1, \ldots, n_{49} \leq K+N$ (provided $0 \leq K < K+N < p$). In particular, each $\lambda$ is represented in the above form for $K = 0$ and some $N$ of the size $N = O\left(p^{8775/8794}\right)$.

One can also derive that for any $\varepsilon > 0$ there exists an integer $r$, such that any residue class $\lambda$ modulo $p$ can be represented in the form $(12)$ with $1 \leq m < p^\varepsilon$ and $1 \leq n, n_1, \ldots, n_r < p$.

We now combine Theorem 1 with the estimate (1) from our work [7] and apply the method Karatsuba [9] of solving multiplicative ternary problems.

For integers $k, \ell, r \geq 0$, $\lambda, L$ and $N$ with $0 \leq L < L + N < p$, we denote by $R_{k,\ell,r}(K, L, S; M, N, T; \lambda)$ the number of solutions of the congruence

$$(m_1! + \ldots + m_k!)(n_1! + \ldots + n_{\ell}!)t_1! \ldots t_r! \equiv \lambda \pmod{p},$$

with $K+1 \leq m_1, \ldots, m_k \leq K+M$, $L+1 \leq n_1, \ldots, n_{\ell} \leq L+N$ and $S+1 \leq t_1, \ldots, t_r \leq S+T$.

**Theorem 7.** Let $K, L, M, N, S$, and $T$, $\lambda$ be integers with $0 \leq K < K+M < p$, $0 \leq L < L+N < p$ and $0 \leq S < S+T < p$ and $\lambda \not\equiv 0 \pmod{p}$. Then for any integers $k, \ell, r \geq 1$, the following bound holds:

$$R_{k,\ell,r}(K, L, S; M, N, T; \lambda) \ll M^{k-1/2+1/(k+1)}N^{\ell-1/2+1/(\ell+1)}T^{3r/4}p^{r/8}(\log p)^{r/4}.$$ 

**Proof.** Let $X$ be the set of multiplicative characters modulo $p$, see [16]. We have an analogue of (1)

$$\sum_{\chi \in \mathcal{X}} \chi(u) = \begin{cases} 0, & \text{if } u \not\equiv 1 \pmod{p}, \\ p-1, & \text{if } u \equiv 1 \pmod{p}. \end{cases} \quad (13)$$
Therefore, we have

\[
R_{k,\ell,r}(K, L, S; M, N, T; \lambda) = \sum_{m_1, \ldots, m_k = K+1}^{K+M} \sum_{n_1, \ldots, n_\ell = L+1}^{L+N} \sum_{t_1, \ldots, t_r = S+1}^{S+T} \frac{1}{p-1} \sum_{\chi \in \chi} \chi \left( (m_1! + \ldots + m_k!) (n_1! + \ldots + n_\ell!) t_1 \ldots t_r \lambda^{-1} \right)
\]

\[
= \frac{1}{p-1} \sum_{\chi \in \chi} \chi^{-1} \left( \sum_{t=S+1}^{S+T} \chi(t) \right)^r \sum_{m_1, \ldots, m_k = K+1}^{K+M} \chi(m_1! + \ldots + m_k!) \sum_{n_1, \ldots, n_\ell = L+1}^{L+N} \chi(n_1! + \ldots + n_\ell!).
\]

Separating the term \(M^k N^\ell T^r/(p-1)\) corresponding to the principal character \(\chi_0\) and then using the bound \(13\) for the sum over \(t\), we obtain

\[
\left| R_{k,\ell,r}(K, L, S; M, N, T; \lambda) - \frac{M^k N^\ell T^r}{p-1} \right| \ll T^{3r/4} p^{r/8} (\log p)^{r/4} \frac{1}{p-1} \sum_{\chi \in \chi} \left| \sum_{m_1, \ldots, m_k = K+1}^{K+M} \chi(m_1! + \ldots + m_k!) \right|^{2}
\]

\[
\cdot \left| \sum_{n_1, \ldots, n_\ell = L+1}^{L+N} \chi(n_1! + \ldots + n_\ell!) \right|.
\]

We see, from \(13\), that

\[
\frac{1}{p-1} \sum_{\chi \in \chi} \left| \sum_{m_1, \ldots, m_k = K+1}^{K+M} \chi(m_1! + \ldots + m_k!) \right|^2 \leq J_k(K, M)
\]

(the above estimate is almost an equality were it not for neglecting the terms with \(m_1! + \ldots + m_k! \equiv 0 \pmod{p}\)). Similarly,

\[
\frac{1}{p-1} \sum_{\chi \in \chi} \left| \sum_{n_1, \ldots, n_\ell = L+1}^{L+N} \chi(n_1! + \ldots + n_\ell!) \right|^2 \leq J_\ell(L, N).
\]
Therefore, by the Cauchy inequality, we see that
\[
\left| R_{k,\ell,r}(K, L, S; M, N, T; \lambda) - \frac{M^k N^\ell T^r}{p-1} \right| \leq T^{3r/4} p^{r/8} (\log p)^{r/4} (J_k(K, M) J_\ell(L, N))^{1/2}.
\]
Using Theorem 1, we finish the proof. \(\square\)

Taking \(M = N = T\), \(k = \ell = 2\) and \(r = 3\) in Theorem 7 we have that any \(\lambda \not\equiv 0 \pmod{p}\) has \(N^7(p-1)^{-1} \left( 1 + O(N^{-17/12} p^{11/8} (\log p)^{3/4}) \right)\) representations of the form
\[
(m_1! + m_2!)(n_1! + n_2!) t_1! t_2! t_3! \equiv \lambda \pmod{p}
\]
with \(K + 1 \leq m_1, m_2, n_1, n_2, t_1, t_2, t_3 \leq K + N\) (provided \(0 \leq K < K + N < p\)). The above asymptotic formula is nontrivial for any fixed \(\varepsilon > 0\) and \(N \geq p^{33/34+\varepsilon}\).

One can also take \(k = 1\), \(\ell = 2\), \(r = 4\) in Theorem 7 and obtain an asymptotic formula for the number of representations of the form
\[
(n_1! + n_2! t_1! t_2! t_3! t_4! t_5! \equiv \lambda \pmod{p}, \tag{14}
\]
with \(K + 1 \leq n_1, n_2, t_1, t_2, t_3, t_4, t_5 \leq K + N\), which becomes nontrivial for \(N \geq p^{18/19+\varepsilon}\). However, our next result provides a stronger bound.

Let us define \(R_{\ell,r}(L, S; N, T; \lambda)\) as the number of solutions of the congruence
\[
(n_1! + \ldots + n_\ell!) t_1! \ldots t_r! \equiv \lambda \pmod{p}
\]
with \(L + 1 \leq n_1, \ldots, n_\ell \leq L + N\) and \(S + 1 \leq t_1, \ldots, t_r \leq S + T\). That is, \(R_{\ell,r}(L, S; N, T; \lambda) = R_{0,\ell,r}(0, L, S; 1, N, T; \lambda)\).

**Theorem 8.** Let \(K, L, M, N, S, T\), \(\lambda\) be integers with \(0 \leq K < K + M < p\), \(0 \leq L < L + N < p\) and \(0 \leq S < S + T < p\) and \(\lambda \not\equiv 0 \pmod{p}\). Then for any integers \(\ell, r \geq 1\) and \(0 \leq s \leq r\), the following bound holds:
\[
R_{\ell,r}(L, S; N, T; \lambda) - \frac{N^\ell T^r}{p-1} \ll N^{\ell-1/2+1/2(\ell+1)} T^{(3r+s)/4-1/2+2^{-s-1}} p^{(r-s)/8} (\log p)^{(r-s)/4}.
\]
Proof. As in the proof of Theorem 8, we derive

\[ R_{\ell,r}(L, S; N, T; \lambda) = \frac{1}{p - 1} \sum_{\chi \in \chi'} \chi(\lambda^{-1}) \left( \sum_{t=S+1}^{S+T} \chi(t) \right)^r \sum_{n_1, \ldots, n_\ell = L+1}^{L+N} \chi(n_1! + \ldots + n_\ell!). \]

Separating the term \( N^T \ell^r/(p - 1) \) corresponding to the principal character \( \chi_0 \), and also then using the bound (1), we obtain

\[ \left| R_{\ell,r}(L, S; N, T; \lambda) - \frac{N^T \ell^r}{p - 1} \right| \ll \sum_{\chi \in \chi', \chi \neq \chi_0} \left| \sum_{t=S+1}^{S+T} \chi(t) \right|^r \sum_{n_1, \ldots, n_\ell = L+1}^{L+N} \chi(n_1! + \ldots + n_\ell!) \]

\[ \ll T^{3(r-s)/4} p^{(r-s)/8} \log p \left( \frac{r-s}{4} \right) \sum_{\chi \in \chi', \chi \neq \chi_0} \left| \sum_{t=S+1}^{S+T} \chi(t) \right|^s \sum_{n_1, \ldots, n_\ell = L+1}^{L+N} \chi(n_1! + \ldots + n_\ell!). \]

Applying the Cauchy inequality, as in the proof of Theorem 8 we derive

\[ \left| R_{\ell,r}(L, S; N, T; \lambda) - \frac{N^T \ell^r}{p - 1} \right| \ll T^{3(r-s)/4} p^{(r-s)/8} \log p \left( \frac{r-s}{4} \right) \left( I_6(S, T) J_6(L, N) \right)^{1/2}, \]

and using (3) together with Theorem 1, we finish the proof. \( \square \)

Taking \( N = T, r = 5, \ell = 2 \) and \( s = 2 \) in Theorem 8, we obtain that any \( \lambda \not\equiv 0 \pmod{p} \) has \( N^T(p - 1)^{-1} \left( 1 + O(N^{-35/24} p^{11/8} \log p)^{3/4} \right) \) representations of the form (4) with \( K + 1 \leq n_1, n_2, t_1, t_2, t_3, t_4, t_5 \leq K + N \) (provided \( 0 \leq K < K + N < p \)), which becomes nontrivial for \( N \geq p^{33/35+\varepsilon} \).

5 Remarks

As we have remarked, a more careful examination of the function \( \kappa(e) \) would lead to a substantial relaxation of the condition \( N^2 \geq M \geq N^{1/2} \) of Theo-
This however, does not affect the most interesting “diagonal” case $M = N$.

Our method can also be used, without any substantial changes, to study the distribution of the products

$$\prod_{j=1}^{n} f(j) \pmod{p}, \quad L + 1 \leq n \leq L + N,$$

where $f(j)$ is rational function (welldefined modulo $p$ for $j = 1, \ldots, p - 1$). In particular, with $f(j) = j^{-1}$ one can estimate exponential sums and the number of solutions of some congruences with ratios of factorials $n!/m!$.

Probably the most challenging open questions are obtaining a nontrivial upper bound on the exponential sums $S_a(L, N)$, and also obtaining an asymptotic formula (or at least a lower bound) on the number of solutions of the Waring-type congruence with factorials

$$n_1! + \ldots + n_\ell! \equiv \lambda \pmod{p},$$

where $L + 1 \leq n_1, \ldots, n_\ell \leq L + N$. Even in the case of $L = 0$, $N = p - 1$ these questions are still unsolved. Theorem 6 seems to be the closest known “approximation” to a full solution of the Waring problem with factorials modulo $p$.

As we have mentioned, our ability to obtain any extensive computational evidences is very limited. So, we dare not make any conjectures about possible answers to the above questions.

References

[1] P. Bürgisser, M. Clausen and M. A. Shokrollahi, *Algebraic complexity theory*, Springer-Verlag, Berlin, 1996.

[2] Q. Cheng, ‘On the ultimate complexity of factorials’, *Proc. 20th Intern. Symp. on Theoretical Aspects of Comp. Sci.*, Lect. Notes in Comp. Sci., Vol. 2607, Springer-Verlag, Berlin, 2003, 157–166.

[3] C. Cobeli, M. Vâjâitu and A. Zaharescu, ‘The sequence $n! \pmod{p}$’, *J. Ramanujan Math. Soc.*, 15 (2000), 135–154.
[4] M. Drmota and R. Tichy, *Sequences, discrepancies and applications*, Springer-Verlag, Berlin, 1997.

[5] P. Erdős and C. Stewart, ‘On the greatest and least prime factors of \(n! + 1\)’, *J. London Math. Soc.* 13 (1976), 513–519.

[6] M. Z. Garaev and F. Luca, ‘On a theorem of A. Sárközy and applications’, *Preprint*, 2003.

[7] M. Z. Garaev, F. Luca and I. E. Shparlinski, ‘Character sums and congruences with \(n!\)’, *Trans. Amer. Math. Soc.*, (to appear).

[8] R. K. Guy, *Unsolved problems in number theory*, Springer-Verlag, New York, 1994.

[9] A. A. Karatsuba, ‘The distribution of products of shifted prime numbers in arithmetic progressions’, *Soviet Math. Dokl.* 11 (1970), 701–711 (in Russian).

[10] A. A. Karatsuba, ‘Fractional parts of functions of a special form’, *Izv. Math.*, 59 (1995), 721-740.

[11] A. A. Karatsuba, ‘Analogues of Kloosterman sums’, *Izv. Math.*, 59 (1995), 971-981.

[12] S. V. Konyagin, ‘Bounds of exponential sums over subgroups and Gauss sums’, *Proc 4th Intern. Conf. Modern Problems of Number Theory and Its Applications*, Moscow Lomonosov State Univ., Moscow, 2002, 86–114 (in Russian).

[13] N. M. Korobov, ‘Estimates of trigonometric sums and their applications’, *Uspehi Mat. Nauk*, 13 (1958), no. 4, 185–192 (in Russian).

[14] N. M. Korobov, ‘Double trigonometric sums and their applications to the estimation of rational sums’, *Math. Notes*, 6 (1969), 472–478.

[15] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, John Wiley, NY, 1974.

[16] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 1997.
[17] F. Luca and I. E. Shparlinski, ‘Prime divisors of shifted factorials’, Bull. Lond. Math. Soc., (to appear).

[18] F. Luca and I. E. Shparlinski, ‘On the largest prime factor of $n! + 2^n - 1$', Preprint, 2003.

[19] F. Luca and P. Stănică, ‘Products of factorials modulo $p$’, Colloq. Math., 96 (2003), 191–205.

[20] B. Rokowska and A. Schinzel, ‘Sur une problème de M. Erdős’, Elem. Math., 15 (1960), 84–85.

[21] M. Shub and S. Smale, ‘On the intractability of Hilbert’s Nullstellensatz and an algebraic version of $P=NP$?’, Duke Math. J., 81 (1995), 47–54.