ON THE VALUE SET OF $n!m!$ MODULO A LARGE PRIME

VICTOR C. GARCÍA

Abstract. We prove that for a large prime number $p$
$$\#(n!m! \pmod p : 1 \leq n, m \leq p) \geq \left(\frac{41}{48} + o(1)\right) p.$$ This improves previously known results from Chen and Dai [1] and Garaev, Luca, and Shparlinski [5].

1. Introduction

The problem of distribution of factorials modulo a prime number $p$ has been a topic of much investigation, see, for example, the recent papers [1]–[7], [10] and references therein. In [8], F11, it is conjectured that about $p/e$ of the residue classes modulo $p$ are missed by the sequence $n!$. If this conjecture were true, the sequence $n!$ modulo $p$ should assume about $(1 - 1/e)p$ distinct values, see [2] for some results of this spirit. This in turn would imply the representability of every residue class modulo $p$ as a product of two factorials. Unconditionally, in [5] it was shown that
$$\#(n!m! \pmod p : 1 \leq n, m \leq p) \geq \frac{5}{6} p + O(p^{1/2} \log^2 p),$$ which has been improved in [1] to
$$\#(n!m! \pmod p : 1 \leq n, m \leq p) \geq \frac{3}{4} p + O(p^{1/2} \log^2 p).$$ In the present paper, using hybrid character sum estimates, we improve this further to the following result.

Theorem (1.1). The following bound holds:
$$\#(n!m! \pmod p : 1 \leq n, m \leq p) \geq \frac{41}{48} p + O(p^{1/2} \log^3 p).$$

2. Proof

Let
$$\mathcal{E} = \{n!m! \pmod p : 1 \leq n, m \leq p\}.$$ The starting point, as in [1, 2, 5], is to employ the congruence
$$\pmod{(2x - 1)! \cdot (p - 2x)!} \equiv 1 \quad (\pmod p),$$ which holds for any positive integer $x \leq p_1$, where $p_1 = (p - 1)/2$.
Let
$$\mathcal{E}_1 = \{2, 4, \ldots, 2p_1\}.$$ Let $\mathcal{E}_2$ be the set of positive odd integers less than $p$ and having the form
$$\pmod{(2x - 1)^r} \quad (\pmod p), \quad 1 \leq x \leq p_1.$$
Here $a^*$ is defined from $aa^* \equiv 1 \pmod{p}$.

Let $\mathcal{E}_3$ be the set of positive odd integers less than $p$ which can be represented in the form $(2z)^* \pmod{p}$, for some $1 \leq z \leq p_1$, and at the same time in the form

$$\frac{(2x)(2x + 1)^*}{p} \equiv 1, \quad \frac{1 - 3x^2}{p} \equiv 1.$$

Here and below $\left( \frac{-}{p} \right)$ is the Legendre symbol. Finally, we define $\mathcal{E}_5$ to be the set of positive odd integers less than $p$ which can be represented in the form $(2z)^* \pmod{p}$ for some $1 \leq z \leq p_1$ and at the same time in the form

$$\frac{(2x - 1)(2x)(2x + 1)^*}{p} \equiv 1, \quad \frac{1 - 3x^2}{p} \equiv 1.$$

For each number of the set $\mathcal{E}_i$, we associate the residue class to which this number belongs. With this convention, since $(2x)!/(p - 2x)! \equiv 2x \pmod{p}$, we have $\mathcal{E}_1 \subset \mathcal{E}$.

If $u \in \mathcal{E}_4$ or $u \in \mathcal{E}_5$, then $u \equiv (2x - 1)^*(2x)^*(2x + 1)^* \pmod{p}$ for some $1 \leq x \leq p_1 - 1$. Together with (2.1) this yields

$$u \equiv (2x - 2)! \cdot (p - 2x - 2)! \pmod{p},$$

whence $u \in \mathcal{E}$. Thus, $\mathcal{E}_4 \subset \mathcal{E}$, $\mathcal{E}_5 \subset \mathcal{E}$. The same argument shows that $\mathcal{E}_2 \subset \mathcal{E}$, $\mathcal{E}_3 \subset \mathcal{E}$.

It is also easy to see that $\mathcal{E}_i \cap \mathcal{E}_j = \emptyset$ for $1 \leq i \neq j \leq 5$. Indeed, if, for example, $u \in \mathcal{E}_3$, then $\left( \frac{4x^2 + 1}{p} \right) = 1$, while if $u \in \mathcal{E}_4 \cup \mathcal{E}_5$, we have $\left( \frac{4x^2 + 1}{p} \right) = -1$. Hence $\mathcal{E}_3 \cap \mathcal{E}_4 = \emptyset$, $\mathcal{E}_3 \cap \mathcal{E}_5 = \emptyset$. The other cases are verified similarly. Therefore,

$$|\mathcal{E}| \geq |\mathcal{E}_1| + |\mathcal{E}_2| + |\mathcal{E}_3| + |\mathcal{E}_4| + |\mathcal{E}_5| = \frac{p - 1}{2} + |\mathcal{E}_2| + |\mathcal{E}_3| + |\mathcal{E}_4| + |\mathcal{E}_5|.$$
In order to estimate \(|E_4|\), we let \(I\) to be the number of solutions of the system of congruences
\[
\begin{align*}
2r - 1 &\equiv (2x - 1)^r(2x)^r(2x + 1)^r \pmod{p} \\
2z &\equiv (2x - 1)(2x)(2x + 1) \pmod{p} \\
\left(\frac{4(2x - 1)(2x + 1) - 1}{p}\right) &\equiv -1 \\
\left(\frac{1 - 3x^2}{p}\right) &\equiv 1
\end{align*}
\]
under the conditions
\[1 \leq x \leq p_1 - 1, \quad 1 \leq z \leq p_1, \quad 1 \leq r \leq p_1.\]
Note that for a given nonzero \(\lambda = 2z \pmod{p}\), if the congruence (2.4)
\[(2x - 1)2x(2x + 1) \equiv \lambda \pmod{p}
\]
has two distinct nonzero solutions \(x \neq y \pmod{p}\), then we have
\[(2y + x)^2 \equiv 1 - 3x^2 \pmod{p}.
\]
This means that given \(r\), the above system of congruence has at most one solution. This implies that \(|E_4| \geq I\).

Let us analyze the cardinality \(|E_5|\). Denote by \(J\) the number of solutions of the system of congruences
\[
\begin{align*}
2r - 1 &\equiv (2x - 1)^r(2x)^r(2x + 1)^r \pmod{p} \\
2z &\equiv (2x - 1)(2x)(2x + 1) \pmod{p} \\
\left(\frac{4(2x - 1)(2x + 1) - 1}{p}\right) &\equiv -1 \\
\left(\frac{1 - 3x^2}{p}\right) &\equiv 1
\end{align*}
\]
with the conditions
\[1 \leq x \leq p_1 - 1, \quad 1 \leq z \leq p_1, \quad 1 \leq r \leq p_1.\]
Given \(r\), we have at most three solutions to this system. Hence, \(|E_5| \geq J/3\), and we have
\[(2.5) \quad |E_4| \geq I, \quad |E_5| \geq \frac{J}{3}.
\]

For \(I\) and \(J\) we will obtain the asymptotic formulas
\[I = \frac{p}{32} + O(p^{1/2} \log^3 p), \quad J = \frac{p}{32} + O(p^{1/2} \log^3 p).
\]
Denote \(g(x) = (2x - 1)2x(2x + 1)\). Using basic trigonometric identities, we obtain
\[I = \frac{1}{p^2} \sum_{a=0}^{p-1} \sum_{b=0}^{p-1} \sum_{x=1}^{p-1} \delta(x)\gamma(x) \sum_{r=1}^{p_1} \sum_{z=1}^{p_1} e^{2\pi i \frac{r}{p} ((2r-1-(g(x))^r)z)} e^{2\pi i \frac{z}{p} (2z-g(x))},
\]
where
\[2\delta(x) = 1 - \left(\frac{4g(x) + 1}{p}\right), \quad 2\gamma(x) = 1 - \left(\frac{1 - 3x^2}{p}\right)\]
we derive
\[ |A| \leq \frac{X+Y}{p} \sum_{a=1}^{p-1} e^{2\pi i an/p} < p \log p, \]

we derive
\[ \left| \frac{1}{p^2} \sum_{a=0}^{p-1} \sum_{x \in A} \delta(x) \gamma(x) \sum_{r=1}^{p_1} \sum_{z=1}^{p_1} e^{2\pi i \frac{x}{p} (2r-1 - (g(x))^r)} e^{2\pi i \frac{z}{p} (2z - g(x))} \right| \leq \frac{1}{p^2} \sum_{a=0}^{p-1} \sum_{b=0}^{p-1} \sum_{r=1}^{p_1} \sum_{z=1}^{p_1} e^{2\pi i \frac{z}{p} r} \left| \sum_{x=1}^{p_1} e^{2\pi i \frac{x}{p} r} \right| \ll \log^2 p. \]

Thus,
\[ I = \frac{1}{p^2} \sum_{a=0}^{p-1} \sum_{b=0}^{p-1} \delta(x) \gamma(x) \sum_{r=1}^{p_1} \sum_{z=1}^{p_1} e^{2\pi i \frac{x}{p} (2r-1 - (g(x))^r)} e^{2\pi i \frac{z}{p} (2z - g(x))} + O(\log^2 p). \]

Separating the term corresponding to \( a = b = 0 \), we obtain
\[ (2.6) \quad I = \frac{p_1}{p^2} \sum_{x=1}^{p_1} \delta(x) \gamma(x) + R_1 + O(\log^2 p) = \frac{P}{32} + R_1 + R_2 + O(\log^2 p), \]

where
\[ (2.7) \quad R_1 \ll \frac{1}{p^2} \sum_{a,b \leq p-1} \sum_{x \neq 0, (a,b) \neq (0,0)} \left| \sum_{r=1}^{p_1} \sum_{z=1}^{p_1} e^{2\pi i \frac{x}{p} (2r-1 - (g(x))^r)} e^{2\pi i \frac{z}{p} (2z - g(x))} \right| S(a, b), \]

\[ S(a, b) = \sum_{x=1}^{p_1} \delta(x) \gamma(x) e^{2\pi i \frac{x}{p} (a(g(x))^* + bg(x))}, \]

\[ R_2 \ll \sum_{x=1}^{p_1} - \left( \frac{4g(x) + 1}{p} \right) - \left( \frac{1 - 3x^2}{p} \right) + \left( \frac{(4g(x) + 1)(1 - 3x^2)}{p} \right). \]

Next, we shall prove that, for \( 0 \leq a, b \leq p - 1 \) with \((a, b) \neq (0, 0), \)
\[ R_1 + R_2 \ll p^{1/2} \log^3 p. \]

Indeed, applying the technique of extending the summation over short intervals to the whole system of residues, we get
\[ S(a, b) = \sum_{x=1}^{p_1} \sum_{y=0}^{p_1} \delta(y) \gamma(y) e^{2\pi i \frac{1}{p} (a(g(y))^* + bg(y))} \frac{1}{p} \sum_{x=0}^{p-1} e^{2\pi i \frac{y}{p} (x-y)} \left| \sum_{x=1}^{p_1} \delta(y) \gamma(y) e^{2\pi i \frac{1}{p} (a(g(y))^* + bg(y)+y)} \right|, \]
where the dash means that from the indicated range of summation over \( y \) the points 0, \( p_1 \) and \( p_1 + 1 \) (which are poles of \( g(y)^* \)) are excluded. Since

\[
4\delta(y)\gamma(y) = 1 - \left( \frac{4g(y) + 1}{p} \right) - \left( \frac{1 - 3y^2}{p} \right) + \left( \frac{(4g(y) + 1)(1 - 3y^2)}{p} \right),
\]

in view of the Weil estimate for hybrid character sums with rational arguments (see, for example, [9]), we have

\[
\left| \sum_{y=0}^{p-1} \delta(y)\gamma(y)e^{2\pi i \frac{1}{2} (a(g(y))^* + bg(y)+ry)} \right| \ll p^{1/2}.
\]

Therefore,

\[
S(a, b) \ll \frac{p^{1/2}}{p} \sum_{r=0}^{p-1} \sum_{x=1}^{p-1} e^{2\pi i \frac{r}{p} x^2} \ll p^{1/2} \log p.
\]

Inserting this into (2.7), we get

\[
R_1 \ll \frac{p^{1/2}}{p^2} \log p \left( \sum_{a=0}^{p-1} \sum_{r=1}^{p} e^{2\pi i \frac{r}{p} a} \right)^2 \ll p^{1/2} \log^3 p.
\]

Similarly, \( R_2 \ll p^{1/2} \log p \). Hence, by (2.6), we obtain that

\[
I = \frac{p}{32} + O(p^{1/2} \log^3 p).
\]

Analogously,

\[
J = \frac{p}{32} + O(p^{1/2} \log^3 p).
\]

Thus, in view of (2.5), we get

\[
|E_4| \geq \frac{p}{32} + O(p^{1/2} \log^3 p), \quad |E_6| \geq \frac{p}{96} + O(p^{1/2} \log^3 p),
\]

which proves the required estimate (2.2).

The same argument applied to \( E_2, E_3 \) implies (2.3). Thus, we conclude that

\[
|E| \geq \left( \frac{1}{2} + \frac{1}{4} + \frac{1}{16} + \frac{1}{32} + \frac{1}{96} \right) p + O(p^{1/2} \log^3 p) = \frac{41}{48} p + O(p^{1/2} \log^3 p).
\]

Acknowledgement

This work was supported by Project PAPIIT IN 100307 from UNAM.

Received December 19, 2006

Final version received February 06, 2007

INSTITUTO DE MATEMÁTICAS
UNIVERSIDAD NACIONAL Autónoma de México
58089, Morelia, Michoacán
México
garci@matmor.unam.mx
REFERENCES


