Monatsh Math (2017) 182:23–31
DOI 10.1007/s00605-015-0867-8

A note on $n!$ modulo p

M. Z. Garaev[1] · **J. Hernández**[1]

Received: 14 September 2015 / Accepted: 19 December 2015 / Published online: 4 January 2016

Abstract Let p be a prime, $\varepsilon > 0$ and $0 < L + 1 < L + N < p$. We prove that if $p^{1/2+\varepsilon} < N < p^{1-\varepsilon}$, then

$$\#\{n! \pmod p;\ \ L+1 \le n \le L+N\} > c(N\log N)^{1/2},\ \ c = c(\varepsilon) > 0.$$

We use this bound to show that any $\lambda \not\equiv 0 \pmod p$ can be represented in the form $\lambda \equiv n_1! \cdots n_7! \pmod p$, where $n_i = o(p^{11/12})$. This refines the previously known range for n_i.

Keywords Factorials · Congruences · Exponential and character sums · Additive combinatorics

Mathematics Subject Classification 11L03 · 11L40 · 11B75 · 11B50

1 Introduction

In what follows, p is a large prime number. For integers L and N with

$$0 < L + 1 < L + N < p$$

Communicated by A. Constantin.

✉ M. Z. Garaev
garaev@matmor.unam.mx

J. Hernández
stgo@matmor.unam.mx

1 Centro de Ciencias Matemáticas, Universidad Nacional Autónoma de México, C.P. 58089 Morelia, Michoacán, Mexico

we consider the set

$$\mathcal{A}(L, N) = \{n! \pmod p;\ \ L+1 \le n \le L+N\}.$$

From the observation

$$\{1\} \cup \{L+2, \dots, L+N\} \pmod p \subset \left\{\frac{a_1}{a_2};\ a_1, a_2 \in \mathcal{A}(L, N)\right\}, \tag{1}$$

it follows that

$$|\mathcal{A}(L, N)| \ge N^{1/2}.$$

In particular, we trivially have $|\mathcal{A}(0, p-1)| \ge (p-1)^{1/2}$. The result of García [8] on the cardinality of product of two factorials modulo p implies that $|\mathcal{A}(0, p-1)| > cp^{1/2}$ for any constant $c < \sqrt{\frac{41}{24}}$ and any sufficiently large prime p. The conjecture is that $|\mathcal{A}(0, p)|$ asymptotically behaves like $(1 - e^{-1})p$, see [5,10].

Improving on the trivial estimate, Klurman and Munsch [11] proved the bound

$$|\mathcal{A}(L, N)| \ge cN^{1/2} \tag{2}$$

with $c = \sqrt{\frac{3}{2}}$ and $p^{1/4+\varepsilon} < N < p$. We note that the condition $N > p^{1/4+\varepsilon}$ can be relaxed, see the remark at the end of the present paper.

Here, using a consequence of Bombieri's bound on exponential sums over algebraic curves, we show that if $p^{1/2+\varepsilon} < N = o(p)$, then the constant c in (2) can be taken arbitrarily large. We then apply this result to the problem of representability of residue classes as a product of seven factorials with small variables.

Further in the text, we use the notation

$$\frac{\mathcal{A}(L, N)}{\mathcal{A}(L, N)} = \left\{\frac{a_1}{a_2};\ a_1, a_2 \in \mathcal{A}(L, N)\right\}.$$

Theorem 1 *For $p^{1/2+\varepsilon} < N < p$, we have the bound*

$$\left|\frac{\mathcal{A}(L, N)}{\mathcal{A}(L, N)}\right| > c_0 N \log(p/N)$$

for some $c_0 = c_0(\varepsilon) > 0$.

From Theorem 1 it follows, in particular, that if $p^{1/2+\varepsilon} < N < p$, then

$$|\mathcal{A}(L, N)| > c_0 (N \log(p/N))^{1/2}$$

for some $c_0 = c_0(\varepsilon) > 0$.

Garaev et al. [7] proved that any $\lambda \not\equiv 0 \pmod p$ can be represented in the form

$$\prod_{i=1}^{7} n_i! \equiv \lambda \pmod p,$$

where $n_i \le c_1 p^{11/12+\varepsilon}$ for some $c_1 = c_1(\varepsilon) > 0$. García [9] improved this condition to $n_i \ll p^{11/12}$. Here and below $A \ll B$ means that $|A| \le cB$ for some constant $c > 0$. Using Theorem 1 we can improve this as follows.

Theorem 2 *Any* $\lambda \not\equiv 0 \pmod p$ *can be represented in the form*

$$\prod_{i=1}^{7} n_i! \equiv \lambda \pmod p,$$

where the positive integers $n_1, \ldots, n_7$ *satisfy*

$$\max\{n_i | i = 1, \ldots, 7\} \ll \frac{p^{11/12}}{(\log p)^{1/2}}.$$

2 Lemmas

We need the following special case of the results of Bombieri [1, Theorem 6] and Chalk and Smith [2, Theorem 2]. As usual, $\mathbb{F}_p$ denotes the field of residue classes modulo p.

Lemma 1 *Let* $(b_1, b_2) \in \mathbb{F}_p \times \mathbb{F}_p$ *be a nonzero vector and let* $f(x, y) \in \mathbb{F}_p[x, y]$ *be a polynomial of degree* $d \ge 1$ *with the following property: there is no* $c \in \mathbb{F}_p$ *for which the polynomial* $f(x, y)$ *is divisible by* $b_1 x + b_2 y + c$. *Then*

$$\left| \sum_{f(x,y)=0} e^{2\pi i (b_1 x + b_2 y)/p} \right| \le 2d^2 p^{1/2}.$$

We remark that the factor 2 on the right hand side can be removed, but it is not essential in our application.

The following lemma is due to Ruzsa, see [12] or [13, Lemma 2.6]. It will be used in the proof of Theorem 2.

Lemma 2 *For any finite nonempty subsets* X, Y, Z *of an abelian group we have*

$$|X - Y| \le \frac{|X + Z||Z + Y|}{|Z|}.$$

In the proof of Theorem 2 we will also need the following estimate of character sums with factorials from the work of García [9, Theorem 3.1].

Lemma 3 *For any positive integer N the following bound holds:*

$$\max_{\chi\neq\chi_0}\left|\sum_{n\le N}\sum_{m\le N}\chi((n+m)!)\right| \ll N^{7/4}p^{1/8}.$$

3 Proof of Theorem 1

By shortening the range of N, if necessary, we can assume that p/N is sufficiently large in terms of ε. Let

$$M = \lfloor \min\{p^{0.1\varepsilon}, (p/N)^{0.1}\}\rfloor.$$

For a positive integer $j \le M$ we define the set

$$X_j = \left\{\prod_{i=1}^{j}(x+L+i) \pmod p; \quad 1 \le x < 0.6N\right\}.$$

Since the polynomial $\prod_{i=1}^{j}(x+L+i)$ has degree j, we have that

$$|X_j| \ge \frac{N}{2j}. \tag{3}$$

Let us prove that for any $j \ge 2$ the following bound holds:

$$\#\{X_j\backslash(X_1\cup\cdots\cup X_{j-1})\} \ge \frac{N}{3j}.$$

Note that

$$\begin{aligned}&\#\{X_j\backslash(X_1\cup\cdots\cup X_{j-1})\}\\ &\quad= \#\{X_j\backslash((X_j\cap X_1)\cup\cdots\cup(X_j\cap X_{j-1}))\}\\ &\quad\ge |X_j| - |X_j\cap X_1| - \cdots |X_j\cap X_{j-1}|.\end{aligned}$$

Therefore, in view of (3) we get

$$\#\{X_j\backslash(X_1\cup\cdots\cup X_{j-1})\} \ge \frac{N}{2j} - |X_j\cap X_1| - \cdots - |X_j\cap X_{j-1}|. \tag{4}$$

We shall now prove that $|X_j\cap X_k| \le N/(6j^2)$ for $1\le k\le j-1$. Let $J(j,k)$ be the number of solutions to the congruence

$$\prod_{i=1}^{j}(x+L+i) \equiv \prod_{i=1}^{k}(y+L+i) \pmod p, \quad 1 \le x, y < 0.6N.$$

Clearly,

$$|X_j \cap X_k| \le J(j,k). \tag{5}$$

Denote

$$f(x,y) = \prod_{i=1}^{j}(x+L+i) - \prod_{i=1}^{k}(y+L+i) \in \mathbb{F}_p[x,y].$$

Following standard arguments, we write $J(j,k)$ in the form

$$\begin{aligned} J(j,k) &= \sum_{\substack{x<0.6N,\ y<0.6N \\ f(x,y)=0}} 1 \\ &\ge \frac{1}{p^2}\sum_{b_1=0}^{p-1}\sum_{b_2=0}^{p-1}\sum_{u<0.6N}\sum_{v<0.6N}\sum_{f(x,y)=0} e^{2\pi i(b_1(x-u)+b_2(y-v))/p}. \end{aligned}$$

From the trivial bound we have that the number of solutions to the equation

$$f(x,y)=0, \quad (x,y)\in\mathbb{F}_p\times\mathbb{F}_p$$

is not greater, than jp. We also recall the elementary estimate

$$\sum_{b=0}^{p-1}\left|\sum_{z<0.6N} e^{2\pi i bz/p}\right| < p\log p,$$

see, for example, the exercises and their solutions in [14, Chapter 3]. Thus, separating the term that corresponds to $b_1=b_2=0$, we obtain

$$J(j,k) \le \frac{jN^2}{p} + (\log p)^2 \max_{(b_1,b_2)}\left|\sum_{f(x,y)=0} e^{2\pi i(b_1x+b_2y)/p}\right|,$$

where the maximum is taken over the integers $0\le b_1, b_2\le p-1$ such that $(b_1,b_2)\ne(0,0)$. Since $j>k\ge 1$, we have that for any $a_1,a_2,a_3\in\mathbb{F}_p$ the polynomials $f(X,a_1X+a_2)$ and $f(a_3,X)$ have degrees j and k respectively in $\mathbb{F}_p[X]$. Therefore, by considering the cases $b_2\ne 0$ and $b_2=0$ separately, it follows that $f(x,y)$ is not divisible by b_1x+b_2y+c in $\mathbb{F}_p[x,y]$. Thus, the condition of Lemma 1 is satisfied. Hence, taking into account that $j\le M$, from Lemma 1 we get

$$J(j,k) \le \frac{jN^2}{p} + O((\log p)^2 j^2 p^{1/2}) \le \frac{N}{6j^2}.$$

This bound and (5) imply that $|X_j \cap X_k| \le N/(6j^2)$. Inserting this into (4), we get that

$$\#\{X_j \backslash (X_1 \cup \cdots \cup X_{j-1})\} \ge \frac{N}{2j} - \frac{(j-1)N}{6j^2} \ge \frac{N}{3j}.$$

Now we observe that

$$X_j \subset \frac{\mathcal{A}(L,N)}{\mathcal{A}(L,N)}, \quad j = 1, 2, \ldots, M.$$

Hence

$$\begin{aligned} \left|\frac{\mathcal{A}(L,N)}{\mathcal{A}(L,N)}\right| &\ge \#\{X_1 \cup X_2 \cup \cdots X_m\} \\ &= |X_1| + \sum_{j=2}^{m} \#\{X_j \backslash (X_1 \cup \cdots \cup X_{j-1})\} \\ &\ge \sum_{j=1}^{M} \frac{N}{3j} \gg N \log M \gg N \log(p/N) \end{aligned}$$

and the result follows.

4 Proof of Theorem 2

Let $p^{0.51} < N < p^{0.99}$. For the brevity, denote $\mathcal{A} = \mathcal{A}(0, N)$. By Theorem 1 we have

$$\left|\frac{\mathcal{A}}{\mathcal{A}}\right| \gg N \log p, \quad |\mathcal{A}| \gg (N \log p)^{1/2}.$$

Application of Lemma 2 in the multiplicative form gives the bound

$$\left|\frac{\mathcal{A}}{\mathcal{A}}\right| \le \frac{|\mathcal{A}\mathcal{A}|^2}{|\mathcal{A}|}.$$

Hence,

$$|\mathcal{A}\mathcal{A}| \ge c_1 (N \log p)^{3/4} \tag{6}$$

for some absolute constant $c_1 > 0$.

Denote $\mathcal{I} = \{1, 2, \ldots, N\}$. Let J be the number of solutions to the congruence

$$(n_1 + m_1)!(n_2 + m_2)!(n_3 + m_3)!xy \equiv \lambda \pmod p,$$

in variables $n_1, n_2, n_3, m_1, m_2, m_3, x, y$ satisfying

$$n_1, n_2, n_3, m_1, m_2, m_3 \in \mathcal{I}, \quad x, y \in \mathcal{A}\mathcal{A}.$$

To prove Theorem 2 it suffices to show that there is a constant $C > 0$ such that $J > 0$ for $N = \lceil Cp^{11/12}(\log p)^{-1/2}\rceil$. We express J via character sums and get

$$J = \frac{1}{p-1}\sum_{\chi}\sum_{n_1,n_2,n_3,m_1,m_2,m_3\in\mathcal{I}}\sum_{x,y\in\mathcal{AA}}\chi((n_1+m_1)!(n_2+m_2)!(n_3+m_3)!xy)\chi(\lambda^{-1}).$$

Separating the term that corresponds to the principal character $\chi = \chi_0$ and following the standard argument we obtain

$$J \geq \frac{N^6|\mathcal{AA}|^2}{p-1} - \frac{1}{p-1}\sum_{\chi\neq\chi_0}\left|\sum_{n,m\in\mathcal{I}}\chi((n+m)!)\right|^3\left|\sum_{x\in\mathcal{AA}}\chi(x)\right|^2.$$

Application of Lemma 3 and the identity

$$\frac{1}{p-1}\sum_{\chi}\left|\sum_{x\in\mathcal{AA}}\chi(x)\right|^2 = |\mathcal{AA}|$$

gives

$$J \geq \frac{N^6|\mathcal{AA}|^2}{p-1} - c_2N^{21/4}p^{3/8}|\mathcal{AA}|,$$

where $c_2 > 0$ is an absolute constant. Using (6) we obtain

$$\begin{aligned} J &\geq \frac{N^{21/4}|\mathcal{AA}|}{p-1}\left(|\mathcal{AA}|N^{3/4} - c_2p^{11/8}\right) \\ &\geq \frac{N^{21/4}|\mathcal{AA}|}{p-1}\left(c_1N^{3/2}(\log p)^{3/4} - c_2p^{11/8}\right). \end{aligned}$$

Hence, taking $N = \lceil 2(c_2/c_1)^{2/3}p^{11/12}(\log p)^{-1/2}\rceil$, we get $J > 0$, which finishes the proof of our theorem.

5 Remarks

As we have mentioned in the introduction, Klurman and Munsch [11] proved that in the range $p^{1/4+\varepsilon} < N < p$ the estimate (2) holds with $c = \sqrt{\frac{3}{2}}$. The condition $N > p^{1/4+\varepsilon}$ can be relaxed using the results from the works [3,4,6]. Indeed, let $N < p^{2/3}$ be sufficiently large. Denote

$$\mathcal{I} = \{L+2, L+3, \ldots, L+N\} \pmod{p}.$$

According to (1) we have

$$\mathcal{I} \subset \frac{\mathcal{A}(L, N)}{\mathcal{A}(L, N)}, \quad \mathcal{I}^{-1} \subset \frac{\mathcal{A}(L, N)}{\mathcal{A}(L, N)}.$$

On the other hand, the results from [6, Theorem 3] or [4, Theorem 1] imply that $|\mathcal{I} \cap \mathcal{I}^{-1}| < N^{1-\delta}$ for some absolute constant $\delta > 0$. Hence,

$$\left|\frac{\mathcal{A}(L, N)}{\mathcal{A}(L, N)}\right| \geq |\mathcal{I} \cup \mathcal{I}^{-1}| = |\mathcal{I}| + |\mathcal{I}^{-1}| - |\mathcal{I} \cap \mathcal{I}^{-1}| \geq 2N - 2 - N^{1-\delta}.$$

Thus, we have $|\mathcal{A}(L, N)| > (\sqrt{2} + o(1))N^{1/2}$ as $N \to \infty$ and $N < p^{2/3}$.

In the proof of Theorem 2 we used the fact that for $N < p^{1-\varepsilon}$ one has

$$|\mathcal{A}(0, N)\mathcal{A}(0, N)| \gg (N \log N)^{3/4}.$$

We note that this bound can significantly be improved for small values of N. For example, let $N < p^{1/2}$. For any positive integers $n, m \leq N$ we have

$$\frac{n}{m} \pmod p \subset \frac{\mathcal{A}(0, N)\mathcal{A}(0, N)}{\mathcal{A}(0, N)\mathcal{A}(0, N)}.$$

Note that in the range $n, m < p^{1/2}$ for distinct rational numbers n/m correspond distinct residue classes $n/m \pmod p$. Therefore,

$$\begin{aligned}\left|\frac{\mathcal{A}(0, N)\mathcal{A}(0, N)}{\mathcal{A}(0, N)\mathcal{A}(0, N)}\right| &\geq \#\left\{\frac{n}{m};\ n, m \in [1, N] \cap \mathbb{Z},\ \gcd(n, m) = 1\right\} \\ &= \left(\frac{6}{\pi^2} + o(1)\right) N^2\end{aligned}$$

as $N \to \infty$. Thus, in the range $N < p^{1/2}$ we have $|\mathcal{A}(0, N)\mathcal{A}(0, N)| \gg N$.

Acknowledgements The authors are grateful to the referee for valuable remarks. M. Z. Garaev was supported by the sabbatical grant from PASPA-DGAPA-UNAM.

References

1. Bombieri, E.: On exponential sums in finite fields. Am. J. Math. **88**, 71–105 (1966)
2. Chalk, J.H.H., Smith, R.A.: On Bombieri's estimate for exponential sums. Acta Arith. **18**, 191–212 (1971)
3. Chang, M.-C., Cilleruelo, J., Garaev, M.Z., Hernández, J., Shparlinski, I.E., Zumalacárregui, A.: Points on curves in small boxes and applications. Michigan Math. J. **63**, 503–534 (2014)
4. Cilleruelo, J., Garaev, M.Z.: Concentration of points on two and three dimensional modular hyperbolas and applications. Geom. Funct. Anal. **21**, 892–904 (2011)
5. Cobeli, C., Vâjâitu, M., Zaharescu, A.: The sequence $n! \pmod p$. J. Ramanujan Math. Soc. **15**, 135–154 (2000)
6. Chan, T.H., Shparlinski, I.: On the concentration of points on modular hyperbolas and exponential curves. Acta Arith. **142**, 59–66 (2010)

7. Garaev, M.Z., Luca, F., Shparlinski, I.E.: Character sums and congruences with n!. Trans. Am. Math. Soc. **356**, 5089–5102 (2004)
8. García, V.C.: On the value set of $n!m!$ modulo a large prime. Bol. Soc. Mat. Mexicana **13**, 1–6 (2007)
9. García, V.C.: Representations of residue classes by product of factorials, binomial coefficients and sum of harmonic sums modulo a prime. Bol. Soc. Mat. Mexicana **14**, 165–175 (2008)
10. Guy, R.K.: Unsolved Problems in Mumber Theory. Springer, New York (1994)
11. Klurman, O., Munsch, M.: Distribution of factorials modulo p (2015). **(Preprint)**. arXiv:1505.01198
12. Ruzsa, I.Z.: On the cardinality of A + A. Colloq. Math. Soc. J. Bolyai 18. Combinatorics (Keszthely, 1976), pp. 933–938
13. Tao, T., Vu, V.: Additive Combinatorics. Cambridge Univ. Press, Cambridge (2006)
14. Vinogradov, I.M.: Elements of Number Theory. Dover Publ, New York (1954)