BULL. AUSTRAL. MATH. SOC. 11B65, 11L40, 11P05
VOL. 71 (2005) [259–264]

WARING PROBLEM WITH FACTORIALS

MOUBARIZ Z. GARAEV, FLORIAN LUCA AND IGOR E. SHPARLINSKI

We show that any residue class λ modulo p can be represented in the form $n_1! + \cdots + n_\ell! \equiv \lambda \pmod p$ with $\ell = O\big((\log p)^3 \log\log p\big)$.

1. INTRODUCTION

Let p be an odd prime. Here, we continue to study exponential sums and various congruences with factorials which have been considered in [**1, 2, 3, 5, 6, 7, 8**] and use some results and methods of [**2, 3**] to study the analogue of the *Waring* problem with factorials.

Namely, let $\ell(p)$ be the smallest integer $\ell \geqslant 1$ such that for every integer λ the congruence

$$n_1! + \cdots + n_\ell! \equiv \lambda \pmod p, \tag{1}$$

has a solution in positive integers $n_1, \ldots, n_\ell$.

THEOREM 1. *For any prime p, $\ell(p) = O\big((\log p)^3 \log\log p\big)$.*

It certainly remains a challenging open question to prove that $\ell(p) = O(1)$, which we believe to be true.

2. PREPARATIONS

Here, we obtain some bounds on the number of solutions of some congruences and some exponential sums. We present them in forms more general that we need in the paper, but which we believe to be of independent interest.

The implied constants in symbols 'O' and '$\ll$' are absolute (we recall that $U \ll V$ and $U = O(V)$ are both equivalent to the inequality $|U| \leqslant cV$ with some constant $c > 0$). In particular, they do not depend on the auxiliary parameter ℓ which occurs in our estimates.

Received 25th October, 2004
During the preparation of this paper, the second author was supported in part by grants SEP-CONACYT 37259-E and 37260-E, and the third author was supported in part by ARC grant DP0211459.

We denote by $J_\ell(N)$ the number of solutions to the congruence

$$\sum_{i=1}^{\ell} n_i! \equiv \sum_{i=\ell+1}^{2\ell} n_i! \pmod p, \qquad 1 \leqslant n_1, \ldots, n_{2\ell} \leqslant N.$$

Our treatment of $J_\ell(N)$ is based on exponential sums. Accordingly, we define

$$\mathbf{e}_p(z) = \exp(2\pi i z/p)$$

and recall the identity (see [9, Exercise 11.a in Chapter 3])

$$\sum_{a=0}^{p-1} \mathbf{e}_p(au) = \begin{cases} 0, & \text{if } u \not\equiv 0 \pmod p, \\ p, & \text{if } u \equiv 0 \pmod p, \end{cases} \tag{2}$$

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

LEMMA 2. *For any positive integers ℓ, N with $\ell < N < p$,*

$$J_\ell(N) \ll \ell^2 N^{2\ell - 1 + 1/(\ell+1)}.$$

PROOF: Let us define exponential sums

$$S_a(N) = \sum_{n=1}^{N} \mathbf{e}_p(an!).$$

The identity (2) implies that

$$J_\ell(N) = \frac{1}{p} \sum_{a=0}^{p-1} \left|S_a(N)\right|^{2\ell}. \tag{3}$$

Put

$$K = \left\lfloor \left(\frac{N^\ell}{\ell!}\right)^{1/(\ell+1)} \right\rfloor.$$

Using the Hölder inequality, we derive

$$\begin{aligned} \left|S_a(p)\right|^{2\ell} &= \left| \sum_{k=1}^{K} \sum_{(k-1)NK^{-1} < m \leqslant kNK^{-1}} \mathbf{e}_p(an!) \right|^{2\ell} \\ &\leqslant K^{2k-1} \sum_{k=1}^{K} \left| \sum_{(k-1)NK^{-1} < m \leqslant kNK^{-1}} \mathbf{e}_p(an!) \right|^{2\ell}, \end{aligned}$$

hence

$$J_\ell(N) \leqslant K^{2\ell-1} G_\ell(K, N),$$

https://doi.org/10.1017/S0004972700038223 Published online by Cambridge University Press

where $G_\ell(K,N)$ is the number of solutions of the congruence

$$\sum_{i=1}^{\ell} m_i! \equiv \sum_{i=\ell+1}^{2\ell} m_i! \pmod p, \qquad 1 \leqslant m_1, \dots, m_{2\ell} \leqslant N,$$

subject to the conditions $|m_i - m_j| < NK^{-1}$ for $1 \leqslant i, j \leqslant 2\ell$.

Obviously, $G_\ell(K,N) \leqslant 2\ell \widetilde{G}_\ell(K,N)$, where $\widetilde{G}_\ell(K,N)$ is number of solutions of the same congruence with the additional restriction that

$$m_1 = \min_{1 \leqslant i \leqslant 2\ell} m_i.$$

To estimate $\widetilde{G}_\ell(K,N)$, we write $m_i = m + t_i$, where $t_1 = 0$ and $0 \leqslant t_i < NK^{-1}$, $2 \leqslant i \leqslant 2\ell$. Then, after dividing by $m_1! \not\equiv 0 \pmod p$, the above congruence takes the form

$$F_{t_1,\dots,t_{2\ell}}(m) \equiv 0 \pmod p, \tag{4}$$

where

$$F_{t_1,\dots,t_{2\ell}}(X) = \sum_{i=1}^{\ell} \prod_{\nu=1}^{t_i} (X+\nu) - \sum_{i=\ell+1}^{2\ell} \prod_{\nu=1}^{t_i} (X+\nu).$$

The polynomial $F_{t_1,\dots,t_{2\ell}}(X)$ vanishes modulo p if and only if the sequence $t_{\ell+1}, \dots, t_{2\ell}$ is a permutation of the sequence $t_1 = 0, t_2, .., t_\ell$. Therefore, this happens for at most $\ell!(NK^{-1}+1)^{\ell-1}$ values of $t_1 = 0, t_2, .., t_{2\ell}$. For these values, the congruence (4) is satisfied for all values of $m = 1, \dots, N$. For the other at most $(NK^{-1}+1)^{2\ell-1}$ values of $t_1 = 0, t_2, .., t_{2\ell}$, the congruence (4) is satisfied for at most $\deg F_{t_1,\dots,t_{2\ell}} \leqslant NK^{-1}+1$ values of m. Hence,

$$\begin{aligned}\widetilde{G}_\ell(K,N) &\leqslant \ell!(NK^{-1}+1)^{\ell-1}N + (NK^{-1}+1)^{2\ell} \\ &= \ell! N^\ell K^{-\ell+1}(1+KN^{-1})^{\ell-1} + N^{2\ell}K^{-2\ell}(1+KN^{-1})^{2\ell}.\end{aligned}$$

We now remark that by our choice of K and the Stirling formula, we have

$$1 + KN^{-1} \leqslant 1 + \left(\frac{N^{-1}}{\ell!}\right)^{1/(\ell+1)} = 1 + O(1/\ell).$$

Therefore,

$$\widetilde{G}_\ell(K,N) \ll \ell! N^\ell K^{-\ell+1} + N^{2\ell}K^{-2\ell},$$

and hence,

$$J_\ell(N) \ll \ell(\ell! N^\ell K^\ell + N^{2\ell}K^{-1}).$$

By our choice of K, we see that

$$\ell! N^\ell K^\ell \leqslant N^{2\ell}K^{-1}$$

https://doi.org/10.1017/S0004972700038223 Published online by Cambridge University Press

and also that for sufficiently large N

$$K \geqslant \left(\frac{N^\ell}{\ell!}\right)^{1/(\ell+1)} - 1 \geqslant \frac{N^{\ell/(\ell+1)}}{2(\ell!)^{1/(\ell+1)}}.$$

Therefore,

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

which finishes the proof. □

For positive integers $k, H, N < p$ we now consider double exponential sums of the form

$$W_a(k; H, N) = \sum_{h=1}^{H} \left| \sum_{n=1}^{N} \mathbf{e}_p(ahn!) \right|^k.$$

We estimate $W_a(k; H, N)$ using essentially the same arguments as in [9, Exercise 14.a in Chapter VI].

LEMMA 3. *For any integer $\ell \geqslant 1$,*

$$\left|W_a(k; H, N)\right| \leqslant \left(pHJ_k(N)\right)^{1/2}.$$

PROOF: Using the Hölder inequality we derive

$$\begin{aligned} \left|W_a(k; H, p)\right|^2 &\leqslant H \sum_{h=1}^{H} \left| \sum_{n=1}^{N} \mathbf{e}_p(ahn!) \right|^{2k} \\ &\leqslant H \sum_{h=1}^{p} \left| \sum_{n=1}^{N} \mathbf{e}_p(ahn!) \right|^{2k} = pHJ_k(N), \end{aligned}$$

which finishes the proof. □

3. PROOF OF THEOREM 1

For some positive integers $s, \ell, H < p$ we denote by T the number of solutions of the congruence

$$\sum_{i=1}^{2s} h_i(n_{i1}! + \cdots + n_{i\ell}!) + \sum_{i=1}^{2\ell} m_i! \equiv \lambda \pmod p,$$

where

$$1 \leqslant n_{1,1}, \ldots, n_{2s,\ell}, m_1, \ldots, m_{2\ell} \leqslant p-1, \qquad 1 \leqslant h_1, \ldots, h_{2s} \leqslant H.$$

By the identity (2), we have

$$T = \frac{1}{p} \sum_{a=0}^{p-1} \left(\sum_{h=1}^{H} \left(\sum_{n=1}^{p} \mathbf{e}_p(ahn!) \right)^\ell \right)^{2s} \left(\sum_{m=1}^{p} \mathbf{e}_p(am!) \right)^{2\ell}.$$

https://doi.org/10.1017/S0004972700038223 Published online by Cambridge University Press

Separating the term $H^{2s}p^{2s\ell+2\ell-1}$ corresponding to $a = 0$, we derive

$$|T - H^{2s}p^{2s\ell+2\ell-1}| \leqslant \frac{1}{p}\sum_{a=1}^{p-1}\left(\sum_{h=1}^{H}\left|\sum_{n=1}^{p}\mathbf{e}_p(ahn!)\right|^{\ell}\right)^{2s}\left|\sum_{m=1}^{p}\mathbf{e}_p(am!)\right|^{2\ell}.$$

Thus, using Lemma 3 and then Lemma 2, we get the inequalities

$$\begin{aligned}|T - H^{2s}p^{2s\ell+2\ell-1}| &\leqslant \frac{1}{p}\big(pHJ_\ell(p)\big)^{s}\sum_{a=1}^{p-1}\left|\sum_{m=1}^{p}\mathbf{e}_p(an!)\right|^{2s}\\ &\leqslant p^{s}H^{s}\big(J_\ell(p)\big)^{s+1} \ll H^{s}\ell^{2s+2}p^{2\ell s+2\ell-1+(s+1)/(\ell+1)}.\end{aligned}$$

Therefore, the inequality

$$T \geqslant H^{2s}p^{2s\ell+2\ell-1} - CH^{s}\ell^{2s+2}p^{2\ell s+2\ell-1+(s+1)/(\ell+1)}$$

holds with some absolute constant $C > 0$. Selecting $\ell = \lfloor \log p \rfloor$, $s = \lfloor \log\log p \rfloor$, and $H = \lceil e^5\ell^2 \rceil$, we see that $T > 0$. Adding, if necessary, several terms of the form $p!$, we see that every residue class λ modulo p can be represented by a sum of the same number $\ell(p)$ of factorials, where $\ell(p) \leqslant 2s\ell H + 2\ell \ll (\log p)^3 \log\log p$. □

4. Remarks

As we have mentioned, the question whether $\ell(p) = O(1)$ remains open. In [4, F11], it is conjectured that the values of $n!$ hit about $(1 - 1/e)p$ of the residue classes modulo p. Proving such a result would immediately imply that $\ell(p) = 2$. Unfortunately this conjecture appears to be very hard.

Our method can also be used, without any substantial changes, to study the Waring problem with more general functions $F(n)$ given by the products

$$F(n) = \prod_{j=1}^{n} f(j) \pmod p,$$

where $f(j)$ is any rational function defined modulo p which has no zeros or poles for all $j = 1, \ldots, p$. In particular, one can easily extend our results to congruences

$$(n_1!)^k + \cdots + (n_\ell!)^k \equiv \lambda \pmod p$$

with a fixed integer $k \geqslant 1$. In fact one can also consider negative values of k.

References

[1] M.Z. Garaev and F. Luca, 'Character sums and products of factorials modulo p', *J. Théor. Nombres Bordeaux* (to appear).

https://doi.org/10.1017/S0004972700038223 Published online by Cambridge University Press

[2] M.Z. Garaev, F. Luca and I.E. Shparlinski, 'Character sums and congruences with $n!$', *Trans. Amer. Math. Soc.* **356** (2004), 5089–5102.

[3] M.Z. Garaev, F. Luca and I.E. Shparlinski, 'Exponential sums and congruences with factorials', *J. Reine Angew. Math.* (to appear).

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

[5] F. Luca and I.E. Shparlinski, 'Prime divisors of shifted factorials', *Bull. Lond. Math. Soc.* (to appear).

[6] F. Luca and I.E. Shparlinski, 'On the largest prime factor of $n! + 2^n - 1$', *J. Théor. Nombres Bordeaux* (to appear).

[7] F. Luca and P. Stănică, 'Products of factorials modulo p', *Colloq. Math.* **96** (2003), 191–205.

[8] C. Stewart, 'On the greatest and least prime factors of $n! + 1$, II', *Publ. Math. Debrecen* **65** (2004), 461–480.

[9] I.M. Vinogradov, *Elements of number theory* (Dover Publications, New York, 1954).

Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58180, Morelia
Michoacán
México
e-mail: garaev@matmor.unam.mx
fluca@matmor.unam.mx

Department of Computing
Macquarie University
Sydney, NSW 2109
Australia
e-mail: igor@ics.mq.edu.au