Journal de Théorie des Nombres
de Bordeaux **17** (2005), 151–160

Character sums and products of factorials modulo p

par Moubariz Z. GARAEV et Florian LUCA

Résumé. Dans cet article, on utilise des estimations de sommes de charactères pour étudier les produits de factorielles modulo p.

Abstract. In this paper, we apply character sum estimates to study products of factorials modulo p.

1. Introduction

In [8], A. Sárközy proved the following Theorem:

Theorem 1.1. *Let p be a prime number, u, v, S, T be integers with $1 \le u,\ v \le p-1$, $1 \le T \le p$. Furthermore, let $C_1,\ C_2,\ \dots,\ C_u$ and $D_1,\ D_2,\ \dots,\ D_v$ be integers with*

$$C_i \not\equiv C_j \pmod p, \qquad \text{for } 1 \le i < j \le u, \tag{1.1}$$

and

$$D_i \not\equiv D_j \pmod p, \qquad \text{for } 1 \le i < j \le v. \tag{1.2}$$

For any integer n, let $f(n)$ denote the number of solutions of

$$C_x \cdot D_y \equiv n \pmod p, \qquad 1 \le x \le u,\ 1 \le y \le v. \tag{1.3}$$

Then,

$$\Big| \sum_{n=S+1}^{S+T} f(n) - \frac{uvT}{p} \Big| < 2(puv)^{1/2} \log(p). \tag{1.4}$$

Our first result in this paper is a modification of the above Theorem 1.1. In what follows, we use $r \ge 1$ for a positive integer. We also use the Vinogradov symbols $\ll$ and $\gg$ and the Landau symbols O and o with their usual meanings.

Theorem 1.2. *Let p be a prime number, u, v, S, T be integers with $1 \le u,\ v \le p-1$, $1 \le T \le p$. Furthermore, let $C_1,\ C_2,\ \dots,\ C_u$ and*

D_1, D_2, ..., D_v be integers satisfying (1.1) *and* (1.2) *above. If $f(n)$ is the function defined at* (1.3) *above, we then have*

(1.5)
$$\sum_{n=S+1}^{S+T} f(n) = \frac{uvT}{p-1} + O_r\left(u+v+(uv)^{1/2}T\left(\frac{p^{1/4}}{T}\right)^{1/r} p^{1/4r^2}\log p\right).$$

For example, when p is large and T is close to $p^{1/4}$, then letting first $\varepsilon > 0$ be any fixed small positive real number, and then choosing r such that $p^{1/4r^2}\log p < p^{\varepsilon}$, we see that the right hand side of (1.5) is of order of magnitude $O_\varepsilon(u+v+p^{1/4+\varepsilon}\sqrt{uv})$, which is better than the right hand side of expression (1.4).

We also provide one application to our Theorem 1.2. In [7], Luca and Stănică put, for every non-negative integers $s \geq t$ and prime number p,

$$P_{s,t}(p) := \left\{\prod_{i=1}^{t} m_i! \pmod p \;\Big|\; \sum_{i=1} m_i = s\right\}, \tag{1.6}$$

and asked for optimal choices for the parameters t and s versus p, such that $P_{s,t}(p)$ covers all the non-zero residue classes modulo p. Theorem 1 in [7] asserts the following:

Theorem 1.3. *Let $\varepsilon > 0$ be arbitrary. There exists a computable positive constant $p_0(\varepsilon)$ such that whenever $p > p_0(\varepsilon)$, then $P_{s,t}(p) \supseteq \mathbb{Z}_p^*$ for all t and s such that $t > p^{\varepsilon}$ and $s - t > p^{1/2+\varepsilon}$.*

We use our Theorem 1.2 to improve the above Theorem 1.3 as follows:

Theorem 1.4. *Let $\varepsilon > 0$ be arbitrary. There exists a computable positive constant $p_0(\varepsilon)$ such that whenever $p > p_0(\varepsilon)$, then $P_{s,t}(p) \supseteq \mathbf{Z}_p^*$ for all t and s such that $t > p^{\varepsilon}$ and $s - t > p^{1/4+\varepsilon}$.*

More information on products of factorials modulo p can be found in the recent papers [1, 3, 4, 5].

Acknowledgements We thank the anonymous refereee for useful comments. Work by both authors was partially supported by Grant SEP-CONACyT 37259-E.

2. The Proofs

The Proof of Theorem 1.2. The proof is based on Karatsuba's method from [6]. In what follows, χ stands for an arbitrary character modulo p, and χ_0

stands for the principal character. Clearly,

$$\sum_{n=S+1}^{S+T} f(n) = \frac{1}{p-1}\sum_{\chi}\sum_{1\le x\le u}\sum_{1\le y\le v}\sum_{n=S+1}^{S+T}\chi(C_xD_y)\overline{\chi}(n) + O(u+v)$$

$$= S_0 + S_1 + O(u+v), \tag{2.1}$$

where

$$S_0 := \frac{1}{p-1}\sum_{1\le x\le u}\sum_{1\le y\le v}\sum_{n=S+1}^{S+T}\chi_0(C_xD_y)\overline{\chi_0}(n), \tag{2.2}$$

and

$$S_1 := \frac{1}{p-1}\sum_{\chi\ne\chi_0}\sum_{1\le x\le u}\sum_{1\le y\le v}\sum_{n=S+1}^{S+T}\chi(C_xD_y)\overline{\chi}(n). \tag{2.3}$$

Clearly,

$$S_0 := \frac{Tuv}{p-1} + O\left(\frac{uv}{p-1} + \frac{Tu}{p-1} + \frac{Tv}{p-1}\right) = \frac{Tuv}{p-1} + O(u+v), \tag{2.4}$$

while

$$S_1 \le \frac{1}{p-1}\sum_{\chi\ne\chi_0}\Big|\sum_{1\le x\le u}\chi(C_x)\Big|\Big|\sum_{1\le y\le v}\chi(D_y)\Big|\Big|\sum_{S+1\le n\le S+T}\chi(n)\Big|$$

$$\le \frac{1}{p-1}\left(\max_{\chi\ne\chi_0}\left\{\Big|\sum_{S+1\le n\le S+T}\chi(n)\Big|\right\}\right)$$

$$\times\sum_{\chi}\Big|\sum_{1\le x\le u}\chi(C_x)\Big|\Big|\sum_{1\le y\le v}\chi(D_y)\Big|. \tag{2.5}$$

By the Cauchy-Schwartz inequality, we have

$$\sum_{\chi}\Big|\sum_{1\le x\le u}\chi(C_x)\Big|\Big|\sum_{1\le y\le v}\chi(D_y)\Big|$$

$$\le \left(\sum_{\chi}\Big|\sum_{1\le x\le u}\chi(C_x)\Big|^2\right)^{1/2}\left(\sum_{\chi}\Big|\sum_{1\le y\le v}\chi(D_y)\Big|^2\right)^{1/2}. \tag{2.6}$$

Note that

$$\sum_{\chi}\Big|\sum_{1\le y\le v}\chi(D_y)\Big|^2=\sum_{\chi}\sum_{\substack{1\le x\le u\\ 1\le x'\le u}}{}'\chi(C_x)\overline{\chi}(C'_x)$$

$$=\sum_{\substack{1\le x\le u\\ 1\le x'\le u}}{}'\sum_{\chi}\chi(C_xC_{x'}^{-1})\le (p-1)u, \tag{2.7}$$

where in the above estimate (2.7) we used $\sum'$ for the sum only over those summation terms which are not zero, as well as the fact that

$$\sum_{\chi}\chi(a)=p-1 \qquad \text{if } a\equiv 1 \pmod p$$

and is zero otherwise, together with the fact that $C_x \not\equiv C_{x'} \pmod p$ if $x\ne x'$ are in $\{1,\dots,u\}$. Inserting (2.7) and its analogue for the set of numbers $\{C_x \mid 1\le x\le u\}$ replaced by the set of numbers $\{D_y \mid 1\le y\le v\}$ into (2.6), we get

$$\sum_{\chi}\Big|\sum_{1\le x\le u}\chi(C_x)\Big|\Big|\sum_{1\le y\le v}\chi(D_y)\Big|\le (p-1)\sqrt{uv}. \tag{2.8}$$

Thus, from (2.5) and (2.8), we have

$$S_1\le \sqrt{uv}\left(\max_{\chi\ne\chi_0}\left\{\Big|\sum_{S+1\le n\le S+T}\chi(n)\Big|\right\}\right), \tag{2.9}$$

and the fact that

$$\max_{\chi\ne\chi_0}\left\{\Big|\sum_{S+1\le n\le S+T}\chi(n)\Big|\right\}\ll T\left(\frac{p^{1/4}}{T}\right)^{1/r}p^{1/4r^2}\log p, \tag{2.10}$$

is just Burgess's character sum estimate from [2]. Inequality (1.5) now follows from (2.1), (2.4), (2.9) and (2.10). □

The Proof of Theorem 1.4. We follow the method of proof of Theorem 1 in [7]. The idea there was to find a suitable list of positive integers $x_1,\ x_2,\ \dots,\ x_t$ consisting of many small numbers, and each one of them repeated a suitable number of times, such that we can modify the element

$$F:=\prod_{i=1}^{t}x_i! \tag{2.11}$$

in enough ways so that to ensure that we can obtain all the congruence classes in $\mathbb{Z}_p^*$. The basic operation by which we can modify the element F shown at (2.11) is given by

(M) *Assume that* $i_1 < i_2 < \cdots < i_j$ *and* $l_1 < l_2 < \cdots < l_j$ *are two disjoints subsets of indices in* $\{1,\ 2,\ \ldots,\ t\}$. *Then,*

$$\left(\prod_{s=1}^{j}(x_{l_s}+1)\right)\left(\prod_{s=1}^{j}x_{i_s}\right)^{-1} F = x_1!\times\cdots\times(x_{l_1}+1)!\times\ldots \\ \cdots\times(x_{i_1}-1)!\times\cdots\times x_t! \\ = F' \in P_{s,t}(p). \tag{2.12}$$

Using (2.12) with $x_{l_1} = \cdots = x_{l_j} = 1$, eliminating the initial number F, and taking inverses in (2.12) above, it suffices to prove the following claim

Claim 2.1. *For any non-negative integers* $s \geq t$ *satisfying the hypothesis of Theorem 1.4, there exist positive integers* $x_1,\ x_2,\ \ldots,\ x_t$ *summing up to* s, *such that every nonzero residue class modulo* p *can be represented by a number of the form*

$$\prod_{r=1}^{j}\left(\frac{x_{i_r}}{2}\right), \tag{2.13}$$

where the subset of indices $\{i_1,\ i_2,\ \ldots,\ i_j\}$ *of* $\{1,\ 2,\ \ldots,\ t\}$ *in* (2.13) *can be any subset such that there exists another subset of* j *indices* $\{l_1,\ l_2,\ \ldots,\ l_j\}$ *disjoint from* $\{i_1,\ i_2,\ \ldots,\ i_j\}$ *for which* $x_{l_r} = 1$ *for all* $r = 1,\ 2,\ \ldots,\ j$.

As in the proof of Theorem 1 in [7], we fix $\varepsilon > 0$, and a positive integer k with $\dfrac{1}{k} < \varepsilon < \dfrac{2}{k}$. From now on, all positive constants $c_1,\ c_2,\ \ldots$, which will appear will be computable and will depend only on k. Since p is assumed to be large, we suppose that $p > 13$. We show that if p is large enough with respect to k, we can then construct a good sublist of numbers $x_1,\ x_2,\ \ldots,\ x_t$ in the following manner:

(1) We first take and repeat exactly two times each of the prime numbers x_i up to $p^{1/k}$.
(2) We then adjoin some even numbers x_j, each one of them smaller than $p^{1/4+1/k}$ but such that the totality of those (counted with multiplicities) does not exceed $c_1 \log\log p$.

(3) The numbers of the form (2.13), where the x_i's are from the lists 1 and 2 and the maximum length j of a product in (2.13) is not more than $2k + 2c_1 \log\log p$ cover the entire $\mathbb{Z}_p^*$.

It is clear that if we can prove the existence of a list satisfying 1–3 above, then we are done. Indeed, we may first adjoin at the sublist consisting of the numbers appearing at 1 and 2 above a number of about $2k+2c_1 \log\log p$ values of x_i all of them equal to 1. The totality of all these numbers (the ones from 1, 2 and these new values of x_i all equal to 1) counted with their multiplicities, so far, is certainly not more than

$$c_2\frac{p^{1/k}}{\log p} + 2k + 4c_1 \log\log p < p^{\varepsilon} - 1 < t - 1, \tag{2.14}$$

while their sum is at most

$$\begin{aligned} c_3\frac{p^{2/k}}{\log p} + 2k + 2c_1 \log\log p + 2c_1 p^{1/4+1/k} \log\log p &< p^{1/4+\varepsilon} - 1 \\ &< s - t - 1, \end{aligned} \tag{2.15}$$

for large p. At this step, we may finally complete the above list with several other values of the x_i equal to 1 until we get a list with precisely $t-1$ numbers, which is possible by inequality (2.14) above, and set the last number of the list to be equal to

$$x_t := s - \sum_{i=1}^{t-1} x_i,$$

which is still positive by inequality (2.15) above.

To prove the existence of a sublist with properties 1–3 above, we proceed as in the proof of Theorem 1 in [7]. We start with the set

$$A := \{n \mid n < p^{1/k} \text{ and } n \text{ is prime}\}. \tag{2.16}$$

The numbers from A will form the sublist mentioned at 1 above but, so far, we take each one of them exactly once. Let

$$B_1 := \left\{ \frac{n_1}{2} \cdot \frac{n_2}{2} \cdot \dots \cdot \frac{n_k}{2} \;\Big|\; n_i \in A,\ n_i \neq n_j \text{ for } 1 \le i \neq j \le k \right\}. \tag{2.17}$$

We first notice that each value of $n \in A$ appears at most k times in an arbitrary product in B_1. We now show that $b_1 := \#B_1$ is large. Indeed, the set B_1 will certainly contain all the numbers of the form

$$\frac{p_1}{2} \cdot \frac{p_2}{2} \cdot \dots \cdot \frac{p_k}{2} = 2^{-k} \cdot p_1 \cdot p_2 \cdot \dots \cdot p_k, \tag{2.18}$$

where p_i is an arbitrary prime subject to the condition

$$p_i \in \left(\frac{p^{1/k}}{2^i},\ \frac{p^{1/k}}{2^{i-1}} \right) \qquad \text{for } i = 1,\ 2,\ \ldots,\ k. \tag{2.19}$$

Notice that the residue classes modulo p of the elements of the form (2.18), where the primes p_i satisfy conditions (2.19), are all distinct. Indeed, the point is that if two of the numbers of the form (2.18) coincide modulo p, then, after cancelling the factor of 2^{-k}, we get two residue classes of integers which coincide modulo p. Now each one of these two integers is smaller than p, therefore if they coincide modulo p, then they must be, in fact, equal. Now the fact that they are all distinct follows from the fact that their prime divisors p_i satisfy condition (2.19). Applying the Prime Number Theorem to estimate from below the number of primes in each one of the intervals appearing in formula (2.19), we get

$$b_1 > c_4 \frac{p}{\log^k p} > \frac{p}{\log^{k+1} p}, \tag{2.20}$$

whenever $p > c_5$. We now construct recursively a (finite) increasing sequence of subsets B_m for $m \geq 1$ in the following way:

Assume that B_m has been constructed and set $b_m := \#B_m$. Assume that $b_m < p-1$ (that is, B_m is not the entire $\mathbb{Z}_p^*$ already). We then have the following trichotomy:

(i) If $b_m \geq p/2$, we then set $B_{m+1} := B_m \cdot B_m$, and notice that $B_{m+1} = \mathbb{Z}_p^*$ and we can no longer continue.

(ii) If $b_m < p/2$ and there exists an even number $a < p^{1/4+1/k}$ such that $a/2 \notin B_m \cdot B_m^{-1}$, we then set $a_m := a$, add a to the list of the x_i's (as one of the numbers from sublist 2 above), and we let

$$B_{m+1} := B_m \cup \frac{a_m}{2} \cdot B_m. \tag{2.21}$$

Notice that

$$b_{m+1} \geq 2b_m. \tag{2.22}$$

(iii) If $b_m < p/2$ and all even numbers a up to $p^{1/4+1/k}$ have the property that $a/2$ is already in $B_m \cdot B_m^{-1}$, we choose the even number a smaller than $p^{1/4+1/k}$ for which the number of representations of $a/2$ of the form $x \cdot y^{-1}$ with $x,\ y \in B_m$ is minimal. We then set $a_m := a$, add a to the list of the x_i's (as one of the numbers from sublist 2 above),

set

$$B_{m+1} := B_m \cup \frac{a_m}{2} \cdot B_m, \tag{2.23}$$

and notice that

$$b_{m+1} \geq \frac{4b_m}{3}. \tag{2.24}$$

In (i)–(iii) above we have used the set-theoretic notation, namely that if U and V are two subsets of $\mathbb{Z}_p^*$, we have denoted by $U \cdot V$ the set of all elements of $\mathbb{Z}_p^*$ of the form $u \cdot v$ with $u \in U$ and $v \in V$, and by U^{-1} the set of all elements of the form u^{-1} for $u \in U$.

We have to justify that (i)–(iii) above do indeed hold. Notice that (i) and (ii) are obvious. The only detail we have to justify is that inequality indeed holds in situation (iii). But for this, we apply our Theorem 1.2 above with $u = v = b_m$, $C_1,\ C_2,\ \ldots,\ C_u$ all the residue classes in B_m and $D_1,\ D_2,\ \ldots,\ D_u$ all the residue classes in B_m^{-1}. We also set $S = 0$ and T to be the largest integer smaller than $p^{1/4+1/k}/2$. Clearly, $T > p^{1/4+1/k}/3$. Since we are discussing situation (iii) above, we certainly have $f(n) \geq 1$ for all positive integers n up to T. Let $M := \min\{f(n) \mid 1 \leq n \leq T\}$, and then $a_m := 2c$, where $f(c) = M$. Denote b_m by b. We apply inequality (1.5) with $r := k$ to get

$$\begin{aligned} M &\leq \frac{b^2}{p-1} + O_k\left(\left(\frac{p^{1/4}}{T}\right)^{1/k} p^{1/4k^2}\log p\right) \\ &= \frac{b^2}{p-1} + O_k\left(p^{1/4+1/4k^2}\log p\right). \end{aligned} \tag{2.25}$$

Let $c_6 := c_6(k)$ be the constant implied in O_k in (2.25) above. We show that the inequality

$$c_6 p^{1/4+1/4k^2}\log p < \frac{b^2}{4p} \tag{2.26}$$

holds for p large enough. Indeed, since $b = b_m \geq b_1 > \dfrac{p}{\log^{k+1} p}$ (by inequality (2.20)), it follows that in order for (2.26) to hold, it suffices that

$$4c_6 \log^{2k+3} p < p^{3/4-1/4k^2}, \tag{2.27}$$

which is certainly satisfied when $p > c_7$. Thus, inequalities (2.25) and (2.26) show that inequality

$$M < \frac{b^2}{p-1} + \frac{b^2}{4p} < \frac{4b^2}{3p} < \frac{2b}{3} \tag{2.28}$$

holds, where the last inequalities in (2.28) follow because $b < p/2$ and $p > 13$. In particular,

$$b_{m+1} = \#(B_m \cup cB_m) \geq b_m + (b_m - M) \geq 2b - \frac{2b}{3} = \frac{4b}{3}, \tag{2.29}$$

which proves inequality (2.24).

The combination of (2.22), (2.23) and (2.24) shows that

$$b_{m+1} > \left(\frac{4}{3}\right)^m b_1 > \left(\frac{4}{3}\right)^m \frac{p}{\log^{k+1} p} \tag{2.30}$$

holds as long as $b_m < p/2$. Now notice that the inequality

$$\left(\frac{4}{3}\right)^m > \frac{\log^{k+1} p}{2} \tag{2.31}$$

will happen provided that $m > c_8 \log\log p$, where one can take $c_8 := \dfrac{k+1}{\log(4/3)}$, for example, and for such large m inequality (2.30) shows that $b_{m+1} > p/2$. In particular, situations (ii) or (iii) above will not occur for more than $c_8 \log\log p$ steps after which we arrive at a point where we apply situation (i) to construct B_{m+1} and we are done. Clearly, (i)–(iii) and the above arguments prove the existence of a sublist of the x_i's satisfying conditions (1)–(3), which finishes the proof of Theorem 1.4.

References

[1] W. Banks, F. Luca, I. E. Shparlinski, H. Stichtenoth, *On the value set of n! modulo a prime*. Turkish J. Math. **29** no. 2 (2005), 169–174.

[2] D. A. Burgess, *On character sums and L-series, II*. Proc. London Math. Soc. (3) **13** (1963), 524–536.

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

[4] M. Z. Garaev, F. Luca, I. E. Shparlinski, *Exponential sums and congruences with factorials*. J. reine angew. Math., to appear.

[5] M. Z. Garaev, F. Luca, I. E. Shparlinski, *Waring problem with factorials mod p*. Bull. Australian Math. Soc. **71** (2005), 259–264.

[6] A. A. Karatsuba, *The distribution of products of shifted prime numbers in arithmetic progressions*. Dokl. Akad. Nauk SSSR **192** (1970), 724–727 (in Russian).

[7] F. Luca, P. Stănică, *Products of factorials modulo p*. Colloq. Math. **96** no. 2 (2003), 191–205.

[8] A. Sárkőzy, *On the distribution of residues of products of integers*. Acta Math. Hung. **49** (3-4) (1987), 397–401.

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

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