ON ASYMPTOTIC DENSITY PROPERTIES OF THE SEQUENCE $(n!)_{n=0}^{\infty}$

L. HAJDU AND Á. PAPP

Dedicated to Robert Tijdeman on the occasion of his 75th birthday.

Abstract. We investigate certain arithmetic properties of factorials. On the one hand, we are interested in the densities of sets of n such that the exponents of given primes in the prime factorization of $n!$ hold certain congruence properties. On the other hand, given M, we investigate the behavior of the M-free parts of factorials. In fact we study the combination of the above two properties. Among others, we show that for any prime p and positive integers a, b, the set of those values of n for which the exponent of p in $n!$ is $\alpha \pmod{p^a}$, and the p-free part of $n!$ is $\beta \pmod{p^b}$, has the expected density for any α, β. In the particular case $p = 2$, $a = 1$, $b = 3$, our results extend and improve a result of Deshouillers and Luca, yielding a better error term for the number of factorials up to x, representable as a sum of three squares.

1. Introduction

It is long known that the equation

$$n! = x^2$$

has no solutions in non-negative integers n, x for $n > 1$. This fact follows e.g. from Bertrand's postulate. Thus the question naturally arises: is it still possible to find infinitely many vales of $n!$, such that the exponents of all $p \in P$ is even, where P is a given finite set of primes? In the case where P consists of the first t primes for some t, this question was posed by Erdős and Graham [10]. The question, and its various extensions have attracted a lot of attention. We consider

2010 *Mathematics Subject Classification.* 11B65, 11B05, 11D85.

Key words and phrases. Factorial, prime factorization, M-free part, sums of three squares.

L.H. was supported in part by grants K115479 and K128088 of the Hungarian National Foundation for Scientific Research and by the projects EFOP-3.6.1-16-2016-00022 and EFOP-3.6.2-16-2017-00015, co-financed by the European Union and the European Social Fund.

the following generalization, which contains all the problems studied earlier.

Problem 1. Let $p_1, \dots, p_t$ be distinct primes, $m_1, \dots, m_t$ be integers greater than 1, and $r_1, \dots, r_t$ be given integers. Set

$$A = A(p_1, \dots, p_t; m_1, \dots, m_t; r_1, \dots, r_t) =$$

$$\{n : \nu_{p_i}(n!) \equiv r_i \pmod{m_i} \ (i = 1, \dots, t)\},$$

where for q being a prime, $\nu_q(k)$ stands for the exponent of q in the prime factorization of the positive integer k. Is it true that for any choice of the parameters p_i, m_i, r_i $(i = 1, \dots, t)$ the set A is non-empty (or even infinite)? Does the set A have a density? Is A relatively dense? (That is, is there an absolute constant c such that the differences of the consecutive elements of A are bounded by c?)

A large part of the above problem is already solved. In the special case where $p_1, \dots, p_t$ are the first t primes, $m_1 = \dots = m_t = 2$ and $r_1 = \dots = r_t = 0$ (i.e. the original question of Erdős and Graham), Problem 1 was answered to the affirmative by Berend [1]. More precisely, Berend showed that in this case A is infinite, and further, it is relatively dense. Berend provided the same result in the case where $m_1 = \dots = m_t$ is arbitrary (still only for $p_1, \dots, p_t$ being the first t primes and $r_1 = \dots = r_t = 0$). Later on, Chen and Zhu [7] formulated Problem 1 in the case $m_i = 2$ with $r_i \in \{0, 1\}$ $(i = 1, \dots, t)$. (In fact they asked only about the relative density of A, but not about its density.) Among other results they proved that (in their settings) either A is empty, or it is infinite and even relatively dense. Sander [20] proved that if $t = 1$, then A is infinite, further, it has a density of 1/2. He also proved that for $t = 2$, A is always infinite. Chen [6] could solve the problem of Chen and Zhu [7] completely, i.e. he proved the relative density of A in Problem 1 with $m_i = 2$ and arbitrary $r_i \in \{0, 1\}$ $(i = 1, \dots, t)$. Problem 1 with arbitrary moduli m_i $(i = 1, \dots, t)$ was first considered by Luca and Stănică [18] (see their Conjecture 2; in fact they did not ask about relative density). They could prove that under the assumption $p_i \nmid m_i$ $(i = 1, \dots, t)$ the density of A exists and it is equal to $1/m_1 \cdots m_t$. Finally, Berend and Kolesnik [2] proved that Conjecture 2 in [17] is true. That is, they showed that the density of A in Problem 1 always exists, and equals to $1/m_1 \cdots m_t$.

We shall also be interested in the behavior of the 'remaining' part of $n!$ (obtained after removing some primes). Later we shall see that this problem (in combination with Problem 1) has an application concerning the set of those integers n for which $n!$ is representable as a sum of three squares. At this point we mention a related, classical question:

what is the distribution of the numbers $1!, 2!, \ldots, (p-1)!$ modulo p, where p is a prime (see F11 in [14])? Answering a question of Erdős, Rokowska and Schinzel [19] showed that if $2!, \ldots, (p-1)!$ are all distinct modulo p, then the missing residue is $-((p-1)/2)!$, and $p \equiv 5 \pmod 8$ must hold; however, there is no such p with $5 < p \leq 1000$. According to a standard conjecture (see F11 of [14] again), approximately p/e modulo p residue classes are not represented by $n!$, as p tends to infinity. This problem has a huge literature; see e.g. the papers [13, 15] and the references given there. For a related question, we also refer to the paper [17].

Problem 2. Let $m > 1$ be a positive integer and take an integer r coprime to m. Set $M = \prod_{p|m} p$ and for any positive integer k, write $k^{(M)}$ for the M-free part of k, that is, set $k^{(M)} := k/\prod_{p|M} p^{\nu_p(k)}$. Put

$$B = B(m; r) = \{n : (n!)^{(M)} \equiv r \pmod m\}.$$

Is it true that for any choice of the integers m, r, the set B is non-empty (or even infinite)? Does the set B have a density? Is B relatively dense?

As a combination of Problems 1 and 2, we also consider

Problem 3. Let $p_1, \ldots, p_t$ be distinct primes, and let $m_1, \ldots, m_t$ and $r_1, \ldots, r_t$ be integers with $m_i \geq 2$ $(i = 1, \ldots, t)$. Further, let $m > 1$ be a positive integer and r be an integer with $\gcd(m, r) = 1$. Put $M = \prod_{p|m} p$. Let

$$C = C(p_1, \ldots, p_t; m_1, \ldots, m_t; r_1, \ldots, r_t; m; r) =$$

$$\{n : \nu_{p_i}(n!) \equiv r_i \pmod{m_i}\ (i = 1, \ldots, t) \text{ and } (n!)^{(M)} \equiv r \pmod m\}.$$

Is it true that for any choice of the parameters $p_1, \ldots, p_t$, $m_1, \ldots, m_t$, $r_1, \ldots, r_t$, m, r the set C is non-empty (or even infinite)? Does the set C have a density? Is C relatively dense?

We think that in case of all the problems, the answers to all the questions are affirmative. In particular, we conjecture that for any choices of the parameters, both sets B and C have densities, and these are given by $1/\varphi(m)$ and $1/m_1 \cdots m_t\varphi(m)$, respectively. (As we mentioned before, the fact that the density of A exists and equals $1/m_1 \cdots m_t$, was proved by Berend and Kolesnik [2].) This would mean that the properties required in the definitions of the sets A and B, are independent. Later on, we shall give some support for this conjecture.

In case of Problems 2 and 3 we know about only very restricted results, which are related to the problem of representing factorials as sums of squares. As we already mentioned, for $n > 1$, Bertrand's postulate implies that $n!$ is never a square. As it was noted by Erdős and Obláth [11], the equation

$$n! = x^2 + y^2$$

has no solutions in non-negative integers n, x, y for $n > 6$. (We have $6! = 720 = 12^2 + 24^2$.) This follows from the fact that for $n \geq 7$ there exists a prime p of the form $4k+3$ between $n/2$ and n (see [4] and [9]). On the other hand, by a classical result of Lagrange we know that the Diophantine equation

$$n! = x^2 + y^2 + z^2 + w^2$$

is solvable for every n, in non-negative integers x, y, z, w. Consider now the remaining case

$$n! = x^2 + y^2 + z^2 \tag{1}$$

in non-negative integers n, x, y, z. By a classical result of Gauss, it is known that an integer is *not* representable as the sum of three squares if and only if it is of the form $2^{2a}(8b+7)$ with non-negative integers a, b. That is, we arrive at Problem 3 with $t = 1$, $p_1 = 2$, $r_1 = 0$, $m = 8$ and $r = 7$. In this particular case, Deshouillers and Luca [8] proved that the set of values of n satisfying (1) has a density of $7/8$. They also provided an asymptotic formula, saying that the number of n with (1) up to N is $(7/8)N + \mathcal{O}(N^{2/3})$. We mention that for the set of positive integers themselves, the corresponding qualitative results are long known. As one can easily check (and it must also be long known, though unfortunately we could not find any related reference), the density of the set of positive integers with even exponents of 2 in their prime factorization, is $2/3$. Further, the density of the set of positive integers having odd part congruent to 7 modulo 8, is clearly $1/4$. So it is not surprising that the set of positive integers *not* representable as the sum of three squares, is $1/6$. The latter statement was proved by Landau [16]. (See Wagstaff [22] for a similar result concerning the Schnirelmann density of the same set.)

As we saw, the question of representing $n!$ as the sum of at most two squares is treated by the knowledge concerning primes in the block of the first n positive integers. The much more general problem of describing the size of the largest prime factor in a block of consecutive integers has been investigated by many authors. For related results, we refer to the excellent, recent survey paper of Shorey and Tijdeman [21], and the references therein.

In this paper we prove several results concerning the most general question formulated, namely Problem 3. We take up the problem where the moduli are any powers of some prime p. We prove that for all choices of the other parameters, the conjecture formulated above is true; that is, in all cases C has the suspected density. We also prove that C is relatively dense, with an explicit bound for the gaps of the consecutive elements of C. In the particular case $p = 2$ and $m_1 = 2$, $m = 8$ we also prove that asymptotically, the error term is $\mathcal{O}(N^{1/2}\log^2 N)$ up to N, thus improving the result of Deshouillers and Luca [8]. In this special case we give a sharp upper bound for the gaps between the consecutive elements of C, as well.

2. Main results

To formulate our general results, we need some notation. Let p be a prime and a, b be positive integers. Put

$$I_1 = \{0, 1, \ldots, p^a - 1\},\ I_2 = \{i\ :\ 1 \le i \le p^b,\ p \nmid i\} \quad \text{and} \quad I = I_1 \times I_2.$$

Observe that $|I| = (p-1)p^{a+b-1}$. To simplify the reference to these sets, by writing $\alpha \in I_1$ and $\beta \in I_2$ for arbitrary integers α and β with $p \nmid \beta$, we shall always mean the elements $\alpha' \in I_1$ and $\beta' \in I_2$, for which $\alpha' \equiv \alpha \pmod{p^a}$ and $\beta' \equiv \beta \pmod{p^b}$, respectively.

In what follows, we shall always assume that p, a, b are fixed. For $(\alpha, \beta) \in I$ put

$$H^{(\alpha,\beta)} = \{n : \nu_p(n!) \equiv \alpha \pmod{p^a},\ (n!)^{(p)} \equiv \beta \pmod{p^b}\}.$$

Finally, we shall use the conventions

$$\nu_p(0) = 0 \quad \text{and} \quad 0^{(p)} = 1.$$

Our first two theorems solves the question of density and relative density in Problem 3 for $t = 1$ with $m_1 = p^a$ and $m = p^b$, where a, b are arbitrary positive integers, $p_1 = p$ is an arbitrary prime, and r_1 and r are arbitrary integers. The following statement shows that the pairs $(\nu_p(n!) \pmod{p^a}, (n!)^{(p)} \pmod{p^b})$ are uniformly distributed among the possible pairs.

Theorem 2.1. *For all $(\alpha, \beta) \in I$, the set $H^{(\alpha,\beta)}$ has a density of $1/(p-1)p^{a+b-1}$.*

In case of relative density, we can even give an explicit upper bound for the differences between the consecutive terms of $H^{(\alpha,\beta)}$.

Theorem 2.2. *For all $(\alpha, \beta) \in I$, the set $H^{(\alpha,\beta)}$ is relatively dense. Further, if we write $H_1^{(\alpha,\beta)} < H_2^{(\alpha,\beta)} < H_3^{(\alpha,\beta)} < \ldots$ for the elements of $H^{(\alpha,\beta)}$, then we have $H_{i+1}^{(\alpha,\beta)} - H_i^{(\alpha,\beta)} \le 2p^{\max(a,b)+b(p-1)p^{a+2b-2}-b+1}$ for all $i \ge 1$.*

As a simple consequence of the above theorems we obtain the following.

Corollary 2.1. *For any* $\alpha \in I_1$ *and* $\beta \in I_2$*, the sets*

$$\{n : \nu_p(n!) \equiv \alpha \pmod{p^a}\} \quad \text{and} \quad \{n : (n!)^{(p)} \equiv \beta \pmod{p^b}\}$$

are relatively dense and are of densities $1/p^a$ *and* $1/(p-1)p^{b-1}$*, respectively.*

Note that the fact that the density of the first set is $1/p^\alpha$, follows from the earlier mentioned results of Berend and Kolesnik [2].

Now we give alike, but more precise statements in the special case of $p = 2$, $a = 1$ and $b = 3$. This case is of particular interest, since it describes the density of the set of values of n for which $n!$ is expressible as a sum of three squares.

The next theorem improves and extends an earlier mentioned result of Deshouillers and Luca [8]. In that paper only the case $(\alpha, \beta) = (0, 7)$ has been investigated (though it seems to be clear that the methods applied in [8] are capable to handle all the other choices of (α, β)). Our result significantly improves the error term $\mathcal{O}(x^{2/3})$ in [8] too.

Theorem 2.3. *Let* $p = 2$*,* $a = 1$*,* $b = 3$ *and* $(\alpha, \beta) \in I$*. Then for all* $x > 0$ *we have*

$$|H^{(\alpha,\beta)} \cap [0, x)| = (1/8)x + \mathcal{O}(x^{1/2} \log^2 x).$$

Our final theorem gives the precise value for the maximal gap length in the sets $H^{(\alpha,\beta)}$ in this special case.

Theorem 2.4. *Let* $p = 2$*,* $a = 1$*,* $b = 3$ *and* $(\alpha, \beta) \in I$*. Then the set* $H^{(\alpha,\beta)}$ *is relatively dense, and if we write* $H_1^{(\alpha,\beta)} < H_2^{(\alpha,\beta)} < H_3^{(\alpha,\beta)} < \dots$ *for the elements of* $H^{(\alpha,\beta)}$*, then we have* $H_{i+1}^{(\alpha,\beta)} - H_i^{(\alpha,\beta)} \leq 42$ *for all* $i \geq 1$*. Further, the upper bound* 42 *is sharp for all* $(\alpha, \beta) \in I$*.*

Remark 1. Clearly, for the special choices $p = 2$, $a = 1$ and $b \leq 3$ Corollary 2.1 also follows from Theorems 2.3 and 2.4.

3. Proofs

To prove our theorems, we need several lemmas. The first lemma reveals a pattern in the behavior of $\nu_p(n!)$. For similar statements and assertions see [7, 20, 17, 2].

Lemma 3.1. *Let* a *be a positive integer. Then for any positive integers* t *and* k *with* $0 \leq t < p$ *and* $k \geq a$ *we have*

$$\nu_p((tp^k + i)!) \equiv \nu_p(i!) + \frac{t}{1-p} \pmod{p^a} \quad (0 \leq i < p^k)$$

with the usual convention $0! = 1$.

Proof. We clearly have

$$\nu_p((tp^k+i)!) = \nu_p\left((tp^k)!\prod_{j=1}^{i}(tp^k+j)\right) \equiv \nu_p((tp^k)!)+\nu_p(i!) \pmod{p^a}.$$

Using the Legendre formula this gives

$$\nu_p((tp^k+i)!) \equiv \nu_p(i!)+t(1+p+\cdots+p^{k-1}) \equiv \nu_p(i!)+t\frac{p^k-1}{p-1} \pmod{p^a},$$

and the lemma follows. □

Our next two lemmas provide similar information about the behavior of $(n!)^{(p)} \pmod{p^b}$.

Lemma 3.2. *Let* $b \geq 1$ *and further assume that* $b \geq 3$ *if* $p = 2$. *Then for any* $k \geq b-1$ *and for any positive integer* t *we have*

$$((tp^k)!)^{(p)} \equiv \begin{cases} ((t2^{b-1})!)^{(2)} \pmod{2^b}, & \text{if } p = 2, \\ (-1)^{t(k-b+1)}((tp^{b-1})!)^{(p)} \pmod{p^b}, & \text{otherwise,} \end{cases}$$

or, shortly

$$((tp^k)!)^{(p)} \equiv (-1)^{t(k-b+1)p}((tp^{b-1})!)^{(p)} \pmod{p^b}$$

for all $p \geq 2$.

Proof. We proceed by induction on k. For $k = b-1$ the statement is an identity. Suppose that the assertion is valid for some $k \geq b-1$. We can write

$$((tp^{k+1})!)^{(p)} = ((tp^k)!)^{(p)} \prod_{\substack{i=1 \\ p\nmid i}}^{tp^{k+1}} i.$$

Since by the induction hypothesis we have

$$((tp^k)!)^{(p)} \equiv \begin{cases} ((t2^{b-1})!)^{(2)} \pmod{2^b}, & \text{if } p = 2, \\ (-1)^{t(k-b+1)}((tp^{b-1})!)^{(p)} \pmod{p^b}, & \text{otherwise,} \end{cases}$$

we only need to show that

$$\prod_{\substack{i=1 \\ p\nmid i}}^{tp^{k+1}} i \equiv \begin{cases} 1 \pmod{2^b}, & \text{if } p = 2, \\ (-1)^t \pmod{p^b}, & \text{otherwise.} \end{cases} \tag{2}$$

To prove this, observe that

$$\prod_{\substack{i=1\\ p\nmid i}}^{tp^{k+1}} i \equiv \left(\prod_{\substack{i=1\\ p\nmid i}}^{p^{k+1}} i\right)^t \pmod{p^{k+1}}.$$

Now in view of $k+1 \geq b \geq 3$ if $p=2$ and $k+1 \geq b \geq 1$ otherwise, we have that $u^2 \equiv 1 \pmod{p^b}$ if and only if $u \equiv \pm 1, 2^k \pm 1 \pmod{2^{k+1}}$ for $p=2$, and $u \equiv \pm 1 \pmod{p^{k+1}}$ for $p \geq 3$. Hence we get

$$\prod_{\substack{i=1\\ p\nmid i}}^{p^{k+1}} i \equiv \begin{cases} 1 \pmod{2^{k+1}}, & \text{if } p=2,\\ -1 \pmod{p^{k+1}}, & \text{otherwise.}\end{cases}$$

This in view of $k+1 \geq b$ gives (2), which proves the lemma. □

The following lemma plays a key role in our arguments.

Lemma 3.3. *Let $b \geq 1$ and $k \geq b-1$. If $p=2$ and $b=2$ then assume that $k \geq b$. Then for every $t \geq 1$ with $p \nmid t$ there exist uniquely determined numbers $\gamma_t(j) \in I_2$ $(1 \leq j \leq p^{b-1})$, such that for all i, j with $(j-1)p^{k-b+1} \leq i < jp^{k-b+1}$, $1 \leq j \leq p^{b-1}$ we have*

$$((tp^k+i)!)^{(p)} \equiv \gamma_t(j)(i!)^{(p)} \pmod{p^b}.$$

Further,

- *i) if $p=2$, then the numbers $\gamma_t(j)$ $(j=1,\dots,2^{b-1})$ form a permutation of I_2 for any odd t,*
- *ii) if $p \geq 3$ then $\gamma_{p-1}(p^{b-1}) = -1$, and the numbers $\gamma_t(j)$ $(1 \leq t \leq p-1,\ 1 \leq j \leq p^{b-1})$ generate the multiplicative group $\mathbb{Z}_{p^b}^*$ of invertible elements of $\mathbb{Z}_{p^b}$.*

Proof. For $p=2$ and $b=1$ the lemma is trivial. Further, if $p=2$ and $b=2$, then the statement can be easily proved by induction; we get $\gamma_1(1)=3$ and $\gamma_1(2)=1$ in this case. So from this point on we shall always assume that if $p=2$ then $b \geq 3$.

First observe that for any s with $tp^k \leq s < (t+1)p^k$ such that $\nu_p(s) \leq k-b$ we have

$$s^{(p)} \equiv (s-tp^k)^{(p)} \pmod{p^b}.$$

This immediately gives that writing

$$\delta_t(j) = \frac{(tp^k+(j-1)p^{k-b+1})^{(p)}}{((j-1)p^{k-b+1})^{(p)}} \quad (1 \leq j \leq p^{b-1})$$

with the convention $0^{(p)} = 1$, we have

$$((tp^k + i)!)^{(p)} \equiv (i!)^{(p)} \delta_t(0) \prod_{\ell=1}^{j} \delta_t(\ell) \pmod{p^b} \tag{3}$$

for all i, j with $(j-1)p^{k-b+1} \le i < jp^{k-b+1}$, $1 \le j \le p^{b-1}$, where $\delta_t(0) = (-1)^{t(k-b+1)p}((tp^{b-1})!)^{(p)}t^{-1}$. Here we used that by Lemma 3.2

$$((tp^k - 1)!)^{(p)} \equiv ((tp^k)!)^{(p)} t^{-1} \equiv (-1)^{t(k-b+1)p}((tp^{b-1})!)^{(p)} t^{-1} \pmod{p^b}.$$

So by choosing

$$\gamma_t(j) \equiv \delta_t(0) \prod_{\ell=1}^{j} \delta_t(\ell) \pmod{p^b} \quad (1 \le j \le p^{b-1}) \tag{4}$$

and noting that these numbers are clearly uniquely determined, the first part of the statement follows.

To prove the second part of the lemma, we have to distinguish the cases $p = 2$ and $p \ge 3$.

The case $p = 2$. To prove the second statement in this case, we show that the $\gamma_t(j)$ are all distinct. This clearly implies i). For this, we need to show that the products $\prod_{\ell=\ell_1}^{\ell_2} \delta_t(\ell)$ are all distinct from 1 modulo 2^b, for $1 < \ell_1 \le \ell_2 \le 2^{b-1}$. (Recall that here we may assume that $b \ge 3$.) Putting $u_{j-1} \equiv ((j-1)^{(2)})^{-1} \pmod{2^b}$ for $j > 1$, we have

$$\delta_t(j) \equiv t2^{b-1-\nu_2(j-1)} u_{j-1} + 1 \pmod{2^b}.$$

Since for any $j > 1$ obviously $\delta_t(j) \not\equiv 1 \pmod{2^b}$, we may assume that $\ell_1 < \ell_2$. Thus we need to show that

$$\prod_{\ell=\ell_1}^{\ell_2} (t2^{b-1-\nu_2(\ell-1)} u_{\ell-1} + 1) \not\equiv 1 \pmod{2^b} \quad (1 < \ell_1 < \ell_2 \le 2^{b-1}).$$

Suppose to the contrary that the above congruence holds for some ℓ_1, ℓ_2 as above. Then for these values of ℓ_1, ℓ_2 we have

$$\prod_{\substack{\ell=\ell_1 \\ 2 \mid \ell-1}}^{\ell_2} (t2^{b-1-\nu_2(\ell-1)} u_{\ell-1} + 1) \prod_{\substack{\ell=\ell_1 \\ 2 \nmid \ell-1}}^{\ell_2} (t2^{b-1-\nu_2(\ell-1)} u_{\ell-1} + 1) \equiv 1 \pmod{2^b}.$$

However, then the same congruence certainly holds also modulo 2^{b-1}. Thus, observing that the second product is clearly 1 modulo 2^{b-1}, in case of $2 \mid \ell - 1$ letting $\ell' - 1 = (\ell - 1)/2$ we get

$$\prod_{\ell'=\lceil(\ell_1+1)/2\rceil}^{\lfloor(\ell_2+1)/2\rfloor} (t2^{b-2-\nu_2(\ell'-1)} u_{\ell'-1} + 1) \equiv 1 \pmod{2^{b-1}}.$$

Here we used that $\nu_2(\ell-1)=\nu_2((\ell-1)/2)+1$ and $((\ell-1)/2)^{(2)}=(\ell-1)^{(2)}$ for $\ell-1$ even, whence $u_{\ell'-1}\equiv u_{\ell-1} \pmod{2^b}$. Since $u_{\ell'-1}\cdot(\ell'-1)^{(2)}\equiv 1 \pmod{2^b}$, we certainly have $u_{\ell'-1}\cdot(\ell'-1)^{(2)}\equiv 1 \pmod{2^{b-1}}$, as well. Finally, observe that $1<\lceil(\ell_1+1)/2\rceil\le\lfloor(\ell_2+1)/2\rfloor\le 2^{b-2}$. Hence our claim that the products $\prod_{\ell=\ell_1}^{\ell_2}\delta_t(\ell)$ $(1<\ell_1\le\ell_2\le 2^{b-1})$ are all different from 1 modulo 2^b follows by induction on b. Thus the products $\prod_{\ell=1}^{j}\delta_t(\ell)$ $(j=1,\dots,2^{b-1})$ are pairwise distinct modulo 2^b. Hence the lemma follows in this case.

The case $p\ge 3$. To prove the second statement in this case, first observe that by Lemma 3.2, (3) and (4) we have

$$(-1)^{k-b+1}((p^{b-1})!)^{(p)}\gamma_{p-1}(p^{b-1})\equiv((p^k)!)^{(p)}\gamma_{p-1}(p^{b-1})\equiv$$
$$\equiv((p^{k+1})!)^{(p)}\equiv(-1)^{k-b+2}((p^{b-1})!)^{(p)}\pmod{p^b}.$$

This gives

$$\gamma_{p-1}(p^{b-1})\equiv -1\pmod{p^b}.$$

Now we construct an element of the subgroup generated by the elements $\gamma_t(j)$ $(1\le t\le p-1,\ 1\le j\le p^{b-1})$ which is a generator of $\mathbb{Z}^*_{p^b}$. In fact we shall prove that already the subgroup G of $\mathbb{Z}^*_{p^b}$ generated by

$$\pm\delta_t(0)\delta_t(1)\quad(1\le t\le p-1)$$

contains such an element. It will be sufficient, since

$$\gamma_{p-1}(p^{b-1})=-1\quad\text{and}\quad\gamma_t(1)=\delta_t(0)\delta_t(1)\quad(1\le t\le p-1).$$

As $\delta_t(1)\equiv t\pmod{p^b}$, we have

$$\pm\delta_t(0)\delta_t(1)\equiv\pm((tp^{b-1})!)^{(p)}\pmod{p^b}\quad(1\le t\le p-1).$$

Observe that for $b=1$ we have $t!\in G$ for all $t=1,\dots,p-1$ implying $G=\mathbb{Z}^*_p$. Let now $b\ge 2$. We show that G contains an element which is generator modulo p^2. As it is well-known, this element will be a generator also modulo p^b. Since by Lemma 3.2 we have

$$((tp^{b-1})!)^{(p)}\equiv\pm((tp)!)^{(p)}\pmod{p^2}$$

for any $b\ge 2$, we need to check the statement only for $b=2$. That is, it is sufficient to show that for $b=2$, the group G contains a generator modulo p^2. For this, first observe that for any t we have

$$\frac{((tp)!)^{(p)}}{(((t-1)p)!)^{(p)}}=t\prod_{i=1}^{p-1}((t-1)p+i)\in G\quad(t=1,\dots,p-1).$$

Recall that if g_1,g_2 are generators modulo p such that

$$g_1\equiv g_2\pmod{p}\quad\text{but}\quad g_1\not\equiv g_2\pmod{p^2},$$

then one of g_1, g_2 is also a generator modulo p^2. Let g be any generator element modulo p with $1 < g < p$. Then by Wilson's theorem we have

$$-g\prod_{i=1}^{p-1}((g-1)p+i) \equiv (p-g)\prod_{i=1}^{p-1}((p-g-1)p+i) \equiv g \pmod{p}.$$

If we would also have

$$-g\prod_{i=1}^{p-1}((g-1)p+i) \equiv (p-g)\prod_{i=1}^{p-1}((p-g-1)p+i) \pmod{p^2},$$

then

$$-g(g-1)\sum_{j=1}^{p-1}\frac{(p-1)!}{j} \equiv (p-1)! + g(g+1)\sum_{j=1}^{p-1}\frac{(p-1)!}{j} \pmod{p}$$

would also hold. However, this by

$$\sum_{j=1}^{p-1}\frac{1}{j} \equiv \sum_{j=1}^{p-1} j \equiv \frac{p(p-1)}{2} \equiv 0 \pmod{p}$$

is impossible. This implies that one of

$$-g\prod_{i=1}^{p-1}((g-1)p+i),\ (p-g)\prod_{i=1}^{p-1}((p-g-1)p+i) \in G$$

is a generator modulo p^2. Hence the lemma follows. □

Remark 2. The combination of Lemmas 3.1 and 3.3 allows us to follow how the classes corresponding to $(\alpha,\beta) \in I$ 'switch'. To see this, just observe that combining these lemmas, for any $k \geq \max(a,b)$ we have that

$$(\nu_p(i!), (i!)^{(p)}) = (\alpha,\beta)$$

if and only if

$$(\nu_p((tp^k+i)!), ((tp^k+i)!)^{(p)}) = \left(\alpha + \frac{t}{1-p}, \gamma_t(j)\beta\right),$$

for any t, j, i with $0 \leq t \leq p-1$, $1 \leq j \leq p^{b-1}$ and $(j-1)p^{k-b+1} \leq i < jp^{k-b+1}$.

Now we can give the proofs of Theorems 2.3 and 2.4.

Proof of Theorem 2.3. First we prove the statement for numbers of the form $x = (2^k)!$. For this, we use linear recurrence sequences of vectors. We need to introduce some notation. For $(\alpha,\beta) \in I$ and $x > y \geq 0$ let

$$H^{(\alpha,\beta)}(y,x) := H^{(\alpha,\beta)} \cap [y,x) \quad \text{and} \quad h^{(\alpha,\beta)}(y,x) := \frac{|H^{(\alpha,\beta)}(y,x)|}{x-y}.$$

n	$2^{\nu_2(n)} \cdot n^{(2)}$	$2^{\nu_2(n!)} \cdot n!^{(2)}$	(α,β)	n	$2^{\nu_2(n)} \cdot n^{(2)}$	$2^{\nu_2(n!)} \cdot n!^{(2)}$	(α,β)
0	1	1	(0,1)	16	2^4	$2^{15} \cdot 3$	(1,3)
1	1	1	(0,1)	17	1	$2^{15} \cdot 3$	(1,3)
2	2	$2 \cdot 1$	(1,1)	18	$2 \cdot 1$	$2^{16} \cdot 3$	(0,3)
3	3	$2 \cdot 3$	(1,3)	19	3	$2^{16} \cdot 1$	(0,1)
4	2^2	$2^3 \cdot 3$	(1,3)	20	$2^2 \cdot 5$	$2^{18} \cdot 5$	(0,5)
5	5	$2^3 \cdot 7$	(1,7)	21	5	$2^{18} \cdot 1$	(0,1)
6	$2 \cdot 3$	$2^4 \cdot 5$	(0,5)	22	$2 \cdot 3$	$2^{19} \cdot 3$	(1,3)
7	7	$2^4 \cdot 3$	(0,3)	23	7	$2^{19} \cdot 5$	(1,5)
8	2^3	$2^7 \cdot 3$	(1,3)	24	$2^3 \cdot 3$	$2^{22} \cdot 7$	(0,7)
9	1	$2^7 \cdot 3$	(1,3)	25	1	$2^{22} \cdot 7$	(0,7)
10	$2 \cdot 5$	$2^8 \cdot 7$	(0,7)	26	$2 \cdot 5$	$2^{23} \cdot 3$	(1,3)
11	3	$2^8 \cdot 5$	(0,5)	27	3	$2^{23} \cdot 1$	(1,1)
12	$2^2 \cdot 3$	$2^{10} \cdot 7$	(0,7)	28	$2^2 \cdot 7$	$2^{25} \cdot 7$	(1,7)
13	5	$2^{10} \cdot 3$	(0,3)	29	5	$2^{25} \cdot 3$	(1,3)
14	$2 \cdot 7$	$2^{11} \cdot 5$	(1,5)	30	$2 \cdot 7$	$2^{26} \cdot 5$	(0,5)
15	7	$2^{11} \cdot 3$	(1,3)	31	7	$2^{26} \cdot 3$	(0,3)

TABLE 1. Exponents of 2 and odd parts of $n!$ for $0 \le n \le 31$.

If $y = 0$, then we shall simply write $H^{(\alpha,\beta)}(x)$ and $h^{(\alpha,\beta)}(x)$, respectively. Define the vectors $\vec{v}_k$ $(k \ge 0)$ by

$$\vec{v}_k := \begin{pmatrix} h^{(0,1)}(2^{k+1}) \\ h^{(0,3)}(2^{k+1}) \\ h^{(0,5)}(2^{k+1}) \\ h^{(0,7)}(2^{k+1}) \\ h^{(1,1)}(2^{k+1}) \\ h^{(1,3)}(2^{k+1}) \\ h^{(1,5)}(2^{k+1}) \\ h^{(1,7)}(2^{k+1}) \end{pmatrix}.$$

Any term of the sequence $(\vec{v}_k)$ for $k \ge 4$ can be expressed by the help of the previous four terms. The initial vectors $\vec{v}_0, \vec{v}_1, \vec{v}_2, \vec{v}_3$ can be easily obtained by the help of Table 1. These are the following:

$$\vec{v}_0 = \begin{pmatrix} 2 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad \vec{v}_1 = \begin{pmatrix} 2 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad \vec{v}_2 = \begin{pmatrix} 2 \\ 1 \\ 1 \\ 0 \\ 1 \\ 2 \\ 0 \\ 1 \end{pmatrix}, \quad \vec{v}_3 = \begin{pmatrix} 2 \\ 2 \\ 2 \\ 2 \\ 1 \\ 5 \\ 1 \\ 1 \end{pmatrix}.$$

As we already mentioned, for every $k \geq 4$ the coordinates of $\vec{v}_k$ can be given by the help of the previous four vectors. The first entry of $\vec{v}_k$, namely $h^{(0,1)}(2^{k+1})$, can be obtained in the following way. We start with

$$h^{(0,1)}(2^{k+1}) = h^{(0,1)}(2^k) + h^{(0,1)}(2^k, 2^{k+1}).$$

Cutting the interval $(2^k, 2^{k+1})$ into four parts, we get

$$h^{(0,1)}(2^{k+1}) = h^{(0,1)}(2^k) + h^{(0,1)}(2^k, 2^k + 2^{k-2}) + h^{(0,1)}(2^k + 2^{k-2}, 2^k + 2^{k-1})$$
$$+ h^{(0,1)}(2^k + 2^{k-1}, 2^k + 2^{k-1} + 2^{k-2}) + h^{(0,1)}(2^k + 2^{k-1} + 2^{k-2}, 2^{k+1}).$$

In what follows, we shall apply Lemmas 3.1 and 3.3 repeatedly, in the way explained in Remark 2. In the latter statement, as one can easily check, now we have

$$(\gamma_1(1), \gamma_1(2), \gamma_1(3), \gamma_1(4)) = (3, 7, 5, 1).$$

We get

$$h^{(0,1)}(2^{k+1}) = h^{(0,1)}(2^k) + h^{(1,3)}(2^{k-2}) + h^{(1,7)}(2^{k-2}, 2^{k-1})$$
$$+ h^{(1,5)}(2^{k-1}, 2^{k-1} + 2^{k-2}) + h^{(1,1)}(2^{k-1} + 2^{k-2}, 2^k).$$

From this we obtain

$$h^{(0,1)}(2^{k+1}) = h^{(0,1)}(2^k) + h^{(1,3)}(2^{k-2}) + \left(h^{(1,7)}(2^{k-1}) - h^{(1,7)}(2^{k-2})\right)$$
$$+ \left(h^{(0,7)}(2^{k-3}) + h^{(0,3)}(2^{k-3}, 2^{k-2})\right) +$$
$$+ \left(h^{(1,1)}(2^k) - h^{(1,1)}(2^{k-1}) - h^{(1,1)}(2^{k-1}, 2^{k-1} + 2^{k-2})\right) =$$
$$= h^{(0,1)}(2^k) + h^{(1,3)}(2^{k-2}) + \left(h^{(1,7)}(2^{k-1}) - h^{(1,7)}(2^{k-2})\right) +$$
$$+ \left(h^{(0,7)}(2^{k-3}) + h^{(0,3)}(2^{k-2}) - h^{(0,3)}(2^{k-3})\right) +$$
$$\left(h^{(1,1)}(2^k) - h^{(1,1)}(2^{k-1}) - h^{(0,3)}(2^{k-3}) - h^{(0,7)}(2^{k-2}) + h^{(0,7)}(2^{k-3})\right).$$

After rearrangement, this yields

$$h^{(0,1)}(2^{k+1}) = h^{(0,1)}(2^k) + h^{(1,1)}(2^k) - h^{(1,1)}(2^{k-1}) +$$
$$+ h^{(1,7)}(2^{k-1}) + h^{(0,3)}(2^{k-2}) - h^{(0,7)}(2^{k-2})$$
$$+ h^{(1,3)}(2^{k-2}) - h^{(1,7)}(2^{k-2}) - 2 \cdot h^{(0,3)}(2^{k-3}) + 2 \cdot h^{(0,7)}(2^{k-3}).$$

Thus the first coordinate of $\vec{v}_k$ is given by

$$\vec{v}_k = (1, 0, 0, 0, 1, 0, 0, 0) \cdot \vec{v}_{k-1} + (0, 0, 0, 0, -1, 0, 0, 1) \cdot \vec{v}_{k-2} +$$
$$+ (0, 1, 0, -1, 0, 1, 0 - 1) \cdot \vec{v}_{k-3} + (0, -2, 0, 2, 0, 0, 0, 0) \cdot \vec{v}_{k-4}.$$

Similar calculations yield the other coordinates of $\vec{v}_k$, as well. Altogether, we get the recurrence relation

$$\vec{v}_k = G_1 \cdot \vec{v}_{k-1} + G_2 \cdot \vec{v}_{k-2} + G_3 \cdot \vec{v}_{k-3} + G_4 \cdot \vec{v}_{k-4} \quad (k \geq 4),$$

where

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix},$$

$$G_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & -1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 \\ -1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$G_3 = \begin{pmatrix} 0 & 1 & 0 & -1 & 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 & 1 & 0 & -1 & 0 \\ 0 & -1 & 0 & 1 & 0 & -1 & 0 & 1 \\ -1 & 0 & 1 & 0 & -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 & 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 & 1 & 0 & -1 & 0 \\ 0 & -1 & 0 & 1 & 0 & -1 & 0 & 1 \\ -1 & 0 & 1 & 0 & -1 & 0 & 1 & 0 \end{pmatrix},$$

$$G_4 = \begin{pmatrix} 0 & -2 & 0 & 2 & 0 & 0 & 0 & 0 \\ -2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & -2 & 0 & 0 & 0 & 0 \\ 2 & 0 & -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -2 & 0 & 2 \\ 0 & 0 & 0 & 0 & -2 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & -2 \\ 0 & 0 & 0 & 0 & 2 & 0 & -2 & 0 \end{pmatrix}.$$

By a theorem of Cerrucci and Vaccarino [5] we know that the above relation can be written as a system of coordinatewise recurrence relations, and the common generating polynomial $g(x)$ of these relations is the characteristic polynomial of the matrix

$$G = \begin{pmatrix} O & O & O & G_4 \\ E & O & O & G_3 \\ O & E & O & G_2 \\ O & O & E & G_1 \end{pmatrix}.$$

Here O is the 8×8 zero matrix, and E is the 8×8 unit matrix. Hence for $g(x)$ we get

$$g(x) = x^{11}(x-2)(x^2+2)(x^4-2x^2+4)(x^4-2x^3+2x^2-4x+4)(x^2-2x+2)^2(x^2-2)^3.$$

Now using the standard theory of recurrence sequences (see e.g. [12]), we get that every coordinate of $\vec{v}_k$ can be written as

$$c_1 2^k + c_2(i\sqrt{2})^k + c_3(-i\sqrt{2})^k + \sum_{i=0}^{3} c_{4+i}\alpha_i^k + \sum_{i=0}^{3} c_{8+i}\beta_i^k +$$
$$(c_{12}k + c_{13})(1+i)^k + (c_{14}k + c_{15})(1-i)^k +$$
$$(c_{16}k^2 + c_{17}k + c_{18})\sqrt{2}^k + (c_{19}k^2 + c_{20}k + c_{21})(-\sqrt{2})^k$$

with complex numbers $c_1, \dots, c_{21}$, which can be different for different coordinates. Here $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ and $\beta_1, \beta_2, \beta_3, \beta_4$ are the (distinct) roots of $x^4 - 2x^2 + 4$ and $x^4 - 2x^3 + 2x^2 - 4x + 4$, respectively. It is easy to check that all these roots have absolute value $\sqrt{2}$. Calculating the vectors $\vec{v}_k$ for $k = 0, \dots, 20$, the constants $c_1, \dots, c_{21}$ can be obtained for each coordinate by solving a system of linear equations. Using Magma [3] we get that $c_1 = 1/8$ in all cases. Thus

$$h^{(\alpha,\beta)}(2^k) = \frac{2^k}{8} + \mathcal{O}\left(k^2\sqrt{2}^k\right) \tag{5}$$

for every $(\alpha, \beta) \in I$. As $k = \log_2 2^k$ and $\sqrt{2}^k = (2^k)^{1/2}$, hence the formula in the theorem follows for $x = 2^k$. As we have

$$h^{(\alpha,\beta)}(2^k, 2^{k+1}) = h^{(\alpha,\beta)}(2^{k+1}) - h^{(\alpha,\beta)}(2^k),$$

thus also

$$h^{(\alpha,\beta)}(2^k, 2^{k+1}) = \frac{2^{k+1}}{8} - \frac{2^k}{8} + \mathcal{O}\left((k+1)^2\sqrt{2}^{k+1}\right) = \frac{2^k}{8} + \mathcal{O}\left(k^2\sqrt{2}^k\right). \tag{6}$$

Let now N be an arbitrary positive integer. Then we can write

$$N = \sum_{i=1}^{j} 2^{f_i},$$

with $f_1 > f_2 > \cdots > f_j \geq 0$. Clearly, $h^{(\alpha,\beta)}(N)$ can be written as

$$h^{(\alpha,\beta)}(N) = h^{(\alpha,\beta)}(2^{f_1}) + h^{(\alpha,\beta)}(2^{f_1}, 2^{f_1} + 2^{f_2}) + \cdots +$$
$$+ h^{(\alpha,\beta)}(2^{f_1} + \cdots + 2^{f_{j-1}}, 2^{f_1} + \cdots + 2^{f_j}).$$

Any term of the above sum can be expressed as

$$h^{(\alpha,\beta)}(2^{f_1} + \cdots + 2^{f_\ell}, 2^{f_1} + \cdots + 2^{f_\ell} + 2^{f_{\ell+1}}) = h^{(\alpha,\beta)}(t2^{f_\ell}, t2^{f_\ell} + 2^{f_{\ell+1}}),$$

where t is odd. By Lemmas 3.1 and 3.3, using (5) and (6), we easily get

$$h^{(\alpha,\beta)}(t2^{f_\ell}, t2^{f_\ell} + 2^{f_{\ell+1}}) = \frac{2^{f_{\ell+1}}}{8} + \mathcal{O}\left(f_{\ell+1}^2\sqrt{2}^{f_{\ell+1}}\right).$$

Thus

$$h^{(\alpha,\beta)}(N) = \left(\frac{2^{f_1}}{8} + \cdots + \frac{2^{f_j}}{8}\right) + \mathcal{O}\left(f_1^2 \sqrt{2}^{f_1}\right) + \cdots + \mathcal{O}\left(f_j^2 \sqrt{2}^{f_j}\right),$$

whence

$$h^{(\alpha,\beta)}(N) = \frac{N}{8} + \mathcal{O}\left(f_1^2 \frac{\sqrt{2}^{f_1+1} - 1}{\sqrt{2}-1}\right) = \frac{N}{8} + \mathcal{O}\left(f_1^2 \sqrt{2}^{f_1}\right).$$

Now using $f_1 \leq \log_2 N$ we get

$$h^{(\alpha,\beta)}(N) = \frac{N}{8} + \mathcal{O}\left(\log^2 N \cdot N^{1/2}\right),$$

and the theorem follows. □

Proof of Theorem 2.4. The assertions can be readily checked. For this purpose, we used simple Magma [3] programs. Checking all the values of $n!$ with $0 \leq n < 127$, we find that all the intervals $[0, 32)$, $[32, 64)$, $[64, 96)$, $[96, 127)$ contain at least two elements from all the sequences $H^{(\alpha,\beta)}$ $((\alpha, \beta) \in I)$. Obviously, the consecutive elements of any $H^{(\alpha,\beta)}$ inside any of these intervals, have distance less than 42. Further, as one can easily check, all the intervals $[0, 14]$, $[21, 31]$, $[32, 48]$, $[47, 63]$, $[64, 78]$, $[85, 95]$, $[96, 122]$, $[100, 127]$ contain at least one element from each $H^{(\alpha,\beta)}$. This immediately shows that all the differences of the consecutive elements below 2^7 inside all the sets $H^{(\alpha,\beta)}$ are bounded by 42. Further, in view of that all the numbers $(127-100)+(14-0)+1$, $(31-21)+(48-32)+1$, $(63-47)+(78-64)+1$, $(95-85)+(122-96)+1$ are at most 42, we also have no problem with merging the four intervals, the first two statements follow by induction using Lemmas 3.1 and 3.3. To see that the bound 42 cannot be improved for any $(\alpha, \beta) \in I$, one can check that

$$(4836, 4878),\ (39652, 39694),\ (2788, 2830),\ (23268, 23310),$$

$$(6884, 6926),\ (740, 782),\ (13028, 13070),\ (19172, 19214)$$

are pairs of consecutive elements of the sets

$$H^{(0,1)},\ H^{(0,3)},\ H^{(0,5)},\ H^{(0,7)},\ H^{(1,1)},\ H^{(1,3)},\ H^{(1,5)},\ H^{(1,7)},$$

respectively. In fact, these are the first instances of pairs of consecutive elements with difference 42 in each $H^{(\alpha,\beta)}$. □

For the proof of Theorem 2.1 we need a further lemma.

Lemma 3.4. *Let p be a prime, u be a positive integer and $a_1, \dots, a_{p^u}$ be real numbers. For $t = 1, \dots, u-1$ put*

$$a_i^{(t)} = \frac{1}{p}\sum_{j=1}^{p} a_{(i-1)p+j}^{(t-1)} \quad (i = 1, \dots, p^{u-t})$$

with $a_i^{(0)} = a_i$ $(i = 1, \dots, p^u)$. Suppose that

$$\max_{1\le i\le p^u} |a_i| > C_1 \tag{7}$$

and

$$|a_{\ell p+j_1}^{(t)} - a_{\ell p+j_2}^{(t)}| \le C_2 \tag{8}$$

for any $0 \le t \le u-1$, $0 \le \ell \le p^{u-t}-1$ and $1 \le j_1 < j_2 \le p$, where C_1 and C_2 are some real numbers with $C_1 > (u+1)(p-1)C_2/p > 0$. Then $a_1, \dots, a_{p^u}$ have the same sign, and we have

$$\min_{1\le i\le p^u} |a_i| > C_1 - (u+1)(p-1)C_2/p.$$

Proof. We proceed by induction on u. For $u = 1$ conditions (7) and (8) reduce to

$$\max(|a_1|, \dots, |a_p|) > C_1 \quad \text{and} \quad |a_{j_1} - a_{j_2}| \le C_2 \quad (1 \le j_1 < j_2 \le p),$$

respectively. These simply yield

$$\min(|a_1|, \dots, |a_p|) > C_1 - C_2 \ge C_1 - 2(p-1)C_2/p,$$

and it is also clear that $a_1, \dots, a_p$ are of the same sign. So the lemma follows in this case. Assume now that the statement is valid for some $u \ge 1$, for any real numbers $a_1, \dots, a_{p^u}$. Take any real numbers $a_1, \dots, a_{p^{u+1}}$, satisfying the properties (7) and (8), with u replaced by $u+1$; in particular, with $C_1 > (u+2)(p-1)C_2/p > 0$. Put

$$b_i = \frac{1}{p}\sum_{j=1}^{p} a_{(i-1)p+j} \quad (i = 1, \dots, p^u).$$

By (7) and (8) we get that

$$|b_{\ell p+j_1} - b_{\ell p+j_2}| \le C_2$$

for all $0 \le \ell \le p^{u-1}-1$ and $1 \le j_1 < j_2 \le p$, whence

$$\max_{1\le i\le p^u} |b_i| > \frac{C_1 + (p-1)(C_1 - C_2)}{p} = C_1 - (p-1)C_2/p.$$

Thus the numbers $b_1, \dots, b_{p^u}$ satisfy the conditions (7) and (8), with C_1 replaced by $C_1 - (p-1)C_2/p$. Hence by the induction hypothesis we have

$$\min_{1\le i\le p^u} |b_i| > C_1 - (u+1)(p-1)C_2/p,$$

and that the b_i-s are of the same sign.

Let i be the index for which $|a_i|$ is minimal. Without loss of generality we may assume that $i = 1$; all the other cases are similar. Then we have

$$C_1 - (u+1)(p-1)C_2/p < |b_1| = \left| \frac{a_1 + \cdots + a_p}{p} \right|.$$

This by (8) immediately gives

$$\min_{1 \le i \le p^{u+1}} |a_i| = |a_1| \ge C_1 - (u+2)(p-1)C_2/p.$$

It is also clear that the a_i-s are of the same sign. Thus the lemma follows. □

Now we are ready to prove Theorems 2.1 and 2.2.

Proof of Theorem 2.1. As in the proof of Theorem 2.3, for $(\alpha, \beta) \in I$ and $x > y \ge 0$ set

$$H^{(\alpha,\beta)}(y, x) = H^{(\alpha,\beta)} \cap [y, x) \quad \text{and} \quad h^{(\alpha,\beta)}(y, x) = \frac{|H^{(\alpha,\beta)}(y, x)|}{x - y}.$$

If $y = 0$, we simply write $H^{(\alpha,\beta)}(x)$ and $h^{(\alpha,\beta)}(x)$, respectively. To prove the theorem, by the above notation we need to show that

$$\lim_{x \to \infty} h^{(\alpha,\beta)}(x) = 1/(p-1)p^{a+b-1}$$

for every $(\alpha, \beta) \in I$. For this, first we prove the following assertion: we have

$$\lim_{k \to \infty} h^{(\alpha,\beta)}((j-1)p^{k-b+1}, jp^{k-b+1}) = 1/(p-1)p^{a+b-1} \tag{9}$$

for any $(\alpha, \beta) \in I$ and $1 \le j \le p^{b-1}$. Note that in particular, this immediately gives

$$\lim_{k \to \infty} h^{(\alpha,\beta)}(p^k) = 1/(p-1)p^{a+b-1}$$

for all $(\alpha, \beta) \in I$. To show (9), for $k \ge \max(a, b)$ and $1 \le j \le p^{b-1}$ set

$$A_j^{(k)} = [(j-1)p^{k-b+1}, jp^{k-b+1}),$$

and for $1 \le t \le p-1$ put

$$B_{t,j}^{(k)} = [tp^k + (j-1)p^{k-b+1}, tp^k + jp^{k-b+1}).$$

Observe that we have

$$A_j^{(k+1)} = \bigcup_{i=(j-1)p}^{(j-1)p+p} A_i^{(k)} \quad (j = 1, \ldots, p^{b-2})$$

and

$$A^{(k+1)}_{tp^{b-2}+j} = \bigcup_{i=(j-1)p}^{(j-1)p+p} B^{(k)}_{t,i} \quad (t = 1, \ldots, p-1,\ j = 1, \ldots, p^{b-2}).$$

Set

$$D(k) = \sum_{(\alpha,\beta)\in I} \sum_{j=1}^{p^{b-1}} (x_j^{(k)}(\alpha,\beta))^2,$$

where

$$x_j^{(k)}(\alpha,\beta) = h^{(\alpha,\beta)}((j-1)p^{k-b+1}, jp^{k-b+1}) - 1/(p-1)p^{a+b-1}.$$

Applying Lemmas 3.1 and 3.3 with $1 \le t \le p-1$, the recursive relation for the sets $A_j^{(k)}$ yields that

$$D(k+1) = \sum_{t=0}^{p-1} \sum_{(\alpha,\beta)\in I} \sum_{j=0}^{p^{b-2}-1} \left(\frac{1}{p} \sum_{i=1}^{p} x^{(k)}_{jp+i}(\alpha^{(t)}_{jp+i}, \beta^{(t)}_{jp+i}) \right)^2 .$$

Here $(\alpha^{(t)}_{jp+i}, \beta^{(t)}_{jp+i}) \in I$ is given by

$$\alpha^{(t)}_{jp+i} + \frac{t}{1-p} \equiv \alpha \pmod{p^a},\ \ \gamma_t(j)\beta^{(t)}_{jp+i} \equiv \beta \pmod{p^b},$$

where the $\gamma_t(j)$ are defined in Lemma 3.3 for $t \ge 1$, and $\gamma_0(j) = 1$. Here one should observe that $\ell \in A_j^{(k)}$ if and only if $tp^k + \ell \in B_{t,j}^{(k)}$, and such an ℓ belongs to $H^{(\alpha^{(t)}_{jp+i},\beta^{(t)}_{jp+i})}((j-1)p^{k-b+1}, jp^{k-b+1})$ if and only if $tp^k+\ell$ belongs to $H^{(\alpha,\beta)}(tp^k + (j-1)p^{k-b+1}, tp^k + jp^{k-b+1})$ $(j = 1, \ldots, p^{b-1})$. Hence, as for all possible values of i, j, t the pairs $(\alpha^{(t)}_{jp+i}, \beta^{(t)}_{jp+i})$ yield permutations of I, by a simple calculation we obtain

(10)

$$D(k)-D(k+1) = \sum_{(\alpha,\beta)\in I} \sum_{j=0}^{p^{b-2}-1} \sum_{1\le i_1<i_2\le p} \left(\frac{x^{(k)}_{jp+i_1}(\alpha,\beta) - x^{(k)}_{jp+i_2}(\alpha,\beta)}{p} \right)^2 .$$

This immediately implies that the sequence $D(k)$ is monotone decreasing. Since clearly, $D(k) \ge 0$ for all k, this sequence is convergent; write σ for its limit. If $\sigma = 0$, then assertion (9) immediately follows. So assume that $\sigma > 0$. Observe that the definition of $D(k)$ implies that for all $k \ge \max(a, b)$ we have

$$m_k := \max_{\substack{(\alpha,\beta)\in I \\ 1\le j\le p^{b-1}}} |x_j^{(k)}(\alpha,\beta)| > \sqrt{\sigma}/p^{a+b}.$$

Now choose a $k \ge \max(a, b)$ such that $D(k) < \sigma + \mu$, where μ is to be chosen later. (For the moment, it is sufficient to consider μ

to be 'very small', also with respect to σ.) Fix j_0 and (α_0, β_0) such that $m_k = |x_{j_0}^{(k)}(\alpha_0, \beta_0)|$. We shall assume that here $x_{j_0}^{(k)}(\alpha_0, \beta_0) > 0$, the other case is completely similar. Observe that by (10) we have that $D(k+i) - D(k+i+1) < \mu$ for all $i \geq 0$. This, choosing μ sufficiently small in terms of σ, by Lemma 3.4 inductively shows that $x_j^{(k)}(\alpha_0, \beta_0) > c_1(\sigma)$ holds for all j with $1 \leq j \leq p^{b-1}$. Here and later on, $c_\ell(\sigma)$ is an explicitly computable positive constant depending only on σ (besides a, b and p, which are considered to be fixed). At this point we need to distinguish two cases.

Assume first that $p = 2$. Then by Lemmas 3.1 and 3.3, using the recursive definition of the sequence $x_j^{(k)}$, together with a similar argument as above (choosing μ to be sufficiently small), we get that there exists a j with $1 \leq j \leq 2^{b-1}$ such that $x_j^{(k+1)}(\alpha_0 - 1, \beta') > c_2(\sigma)$, and then that in fact $x_j^{(k+1)}(\alpha_0 - 1, \beta') > c_3(\sigma)$ for all j with $1 \leq j \leq 2^{b-1}$, where $\beta' \in I_2$. Repeating the argument, we get that for all $\alpha^* \in I_1$ there exists a $\beta^* \in I_2$ such that $x_j^{(k+2^a)}(\alpha^*, \beta^*) > c_4(\sigma)$ for all j with $1 \leq j \leq 2^{b-1}$. Now let $(\hat{\alpha}, \hat{\beta}) \in I$ be arbitrary. Then there exists a $\beta^* \in I_2$ such that $x_j^{(k+2^a)}(\hat{\alpha} + 1, \beta^*) > c_4(\sigma)$. Then, since the $\gamma_1(j)$ in Lemma 3.3 yield a permutation of the invertible elements of $\mathbb{Z}_{2^b}$, we see that for the index j defined by $\gamma_1(j)\beta^* \equiv \hat{\beta} \pmod{2^b}$, with the usual argument we obtain that $x_j^{(k+2^a+1)}(\hat{\alpha}, \hat{\beta}) > c_5(\sigma)$. Then repeating the argument once more, we get that in fact $x_j^{(k+2^a+1)}(\hat{\alpha}, \hat{\beta}) > c_6(\sigma)$ for all j with $1 \leq j \leq 2^{b-1}$. This is already sufficient for our purposes; we shall draw the conclusion a bit later, after examining the case of odd primes p as well.

So let now p be an odd prime. Recall that $x_j^{(k)}(\alpha_0, \beta_0) > c_1(\sigma)$ for all j with $1 \leq j \leq p^{b-1}$, and let $\beta^* \in I_2$ be arbitrary. By Lemma 3.3 there exists an ℓ depending only on p and b, and $\gamma_{t_1}(j_1), \dots, \gamma_{t_\ell}(j_\ell) \in I_2$ such that $\gamma_{t_1}(j_1) \cdots \gamma_{t_\ell}(j_\ell)\beta_0 \equiv \beta^* \pmod{p^b}$. This by the usual argument gives that for every $\beta^* \in I_2$ one can find an $\alpha^* \in I_1$ such that $x_j^{(k+s)}(\alpha^*, \beta^*) > c_7(\sigma)$ for all j with $1 \leq j \leq p^{b-1}$, with some $s \geq 0$ depending only on p and b. Now applying Lemmas 3.1 and 3.3 with $t = p - 1$ and $j = p^b - 1$, by the usual argument again, we get that $x_j^{(k+s+1)}(\alpha^* - 1, -\beta^*) > c_8(\sigma)$ for all j with $1 \leq j \leq p^{b-1}$. Repeating this argument $2p^a$ times, since p^a is odd, we get that $x_j^{(k+s+2p^a)}(\alpha, \beta^*) > c_9(\sigma)$ for all $\alpha \in I_1$ and for all j with $1 \leq j \leq p^{b-1}$. Since $\beta^* \in I_2$ is arbitrary, we get that in fact $x_j^{(k+s')}(\hat{\alpha}, \hat{\beta}) > c_{10}(\sigma)$ for all $(\hat{\alpha}, \hat{\beta}) \in I$ and j with $1 \leq j \leq p^{b-1}$, for some $s' \geq 0$ depending only on a, b and p.

So in both cases we get $x_j^{(k+s')}(\hat{\alpha},\hat{\beta}) > c_{11}(\sigma)$ for all $(\hat{\alpha},\hat{\beta}) \in I$ and j with $1 \le j \le p^{b-1}$, for some $s' \ge 0$ depending only on a, b and p. However, this contradicts the identity

$$\sum_{(\alpha,\beta)\in I} x_j^{(k)}(\alpha,\beta) = 0$$

being valid for all $k \ge \max(a,b)$ and $1 \le j \le p^{b-1}$. This proves that $\sigma = 0$, and consequently, $\lim_{k\to\infty} m_k = 0$ (hence also (9)).

Now choose an arbitrary $\varepsilon > 0$, and let $k_0 \ge \max(a,b)$ be such that

$$\left| h^{(\alpha,\beta)}((j-1)p^{k-b+1}, jp^{k-b+1}) - \frac{1}{|I|} \right| < \varepsilon \tag{11}$$

whenever $k \ge k_0$, for any $(\alpha,\beta) \in I$ and $1 \le j \le p^{b-1}$. By (9) we know that such a k_0 exists. In fact (11) is valid for any $j \ge 1$. This follows by induction from the fact that by Lemmas 3.1 and 3.3, for any $k \ge k_0$ we have

$$H^{(\alpha,\beta)}(tp^k+(j-1)p^{k-b+1}, tp^k+jp^{k-b+1}) = H^{(\alpha',\beta')}((j-1)p^{k-b+1}, jp^{k-b+1}),$$

with some $(\alpha',\beta') \in I$ and t, j with $0 \le t \le p-1$ and $1 \le j \le p^{b-1}$.

Let N_0 be a positive integer to be specified later, and let $N > N_0$. Write

$$N = \sum_{s=1}^{r} c_s p^{f_s}$$

with integers $f_1 > \cdots > f_s \ge 0$ and $0 < c_1, \ldots, c_s < p$. Then for any $(\alpha,\beta) \in I$ we can clearly write

(12)

$$\left|H^{(\alpha,\beta)}(N)\right| = \sum_{\ell=1}^{r} \sum_{i=0}^{c_\ell - 1} \left| H^{(\alpha,\beta)} \left(\sum_{g=1}^{\ell-1} c_g p^{f_g} + ip^{f_\ell}, \sum_{g=1}^{\ell-1} c_g p^{f_g} + (i+1)p^{f_\ell} \right) \right|.$$

Let M be the largest multiple of p^{k_0-b+1} with $M \le N$, and set $q = M/p^{k_0-b+1}$. Using (11), for every $1 \le j \le q$ we have

$$\frac{1}{|I|} - \varepsilon < \frac{\left|H^{(\alpha,\beta)}((j-1)p^{k-b+1}, jp^{k-b+1})\right|}{p^{k-b+1}} < \frac{1}{|I|} + \varepsilon,$$

whenever $k \ge k_0$. Write

$$N = \sum_{s=1}^{r} c_s p^{f_s} = \sum_{s=1}^{r'} c_s p^{f_s} + T,$$

where $T = N - M$; observe that $0 \leq T < p^{k_0-b+1}$. Thus, using (11), we have both

$$|H^{(\alpha,\beta)}(N)| \leq \sum_{s=1}^{r'} c_s \left(\frac{p^{f_s}}{|I|} + \varepsilon p^{f_s}\right) + T \leq \frac{N-T}{|I|} + \varepsilon(N-T) + T,$$

and

$$|H^{(\alpha,\beta)}(N)| \geq \sum_{s=1}^{r'} c_s \left(\frac{p^{f_s}}{|I|} - \varepsilon p^{f_s}\right) \geq \frac{N-T}{|I|} - \varepsilon(N-T).$$

Recalling that $h^{(\alpha,\beta)}(N) = |H^{(\alpha,\beta)}(N)|/N$, taking N_0 sufficiently large, the theorem follows. □

Proof of Theorem 2.2. The statement that for any $(\alpha, \beta) \in I$, $H^{(\alpha,\beta)}$ is relatively dense, would follow from the arguments given in the proof of Theorem 2.1 (in particular, from (9)). However, to give an explicit bound for the largest gap in $H^{(\alpha,\beta)}$, we follow another (though similar) method.

From the proof of Theorem 2.1, for $k \geq \max(a, b)$ we extend the notation

$$A_j^{(k)} = [(j-1)p^{k-b+1}, jp^{k-b+1})$$

from $1 \leq j \leq p^{b-1}$ to $1 \leq j \leq p^b$. For all such j, set

$$T_j^{(k)} = \{(\alpha, \beta) \in I : H^{(\alpha,\beta)} \cap A_j^{(k)} \neq \emptyset\}.$$

Observe that by Lemmas 3.1 and 3.3 (see also Remark 2), $T_{tp^{b-1}+j}^{(k)}$ is an injective map of $T_j^{(k)}$, for $t = 0, \dots, p-1$ and $j = 1, \dots, p^{b-1}$. Further, for any $k \geq \max(a, b)$ we clearly have

$$T_j^{(k+1)} = \bigcup_{i=1}^{p} T_{(j-1)p+i}^{(k)} \quad (j = 1, \dots, p^{b-1}).$$

For k as before, let

$$s^{(k)} = |T_1^{(k)}| + \dots + |T_{p^{b-1}}^{(k)}|.$$

Clearly, $s^{(k)}$ is a positive integer with $s^{(k)} \leq p^{b-1}|I| = (p-1)p^{a+2b-2}$. From what we know about the sets $T^{(k)}$ and $T^{(k+1)}$, we easily deduce that $s^{(k+1)} \geq s^{(k)}$, with equality precisely when $T_{(j-1)p+i_1}^{(k)} = T_{(j-1)p+i_2}^{(k)}$ for all $j = 1, \dots, p^{b-1}$ and $1 \leq i_1 < i_2 \leq p$. Using this observation together with the inductive definition of the sets $T_j^{(k)}$, we see that if for some k we have

$$s^{(k)} = s^{(k+1)} = \dots = s^{(k+b)},$$

then in fact

$$T_{j_1}^{(k)} = T_{j_2}^{(k)} \quad (1 \le j_1 < j_2 \le p^b).$$

This implies that then, with this k, we have $s^{(k+\ell)} = s^{(k)}$, for all $\ell \ge 0$. Summarizing the above arguments, we obtain that there exists a K such that $s^{(K+\ell)} = s^{(K)}$ for all $\ell \ge 0$, and that

$$K = \max(a, b) + b(p-1)p^{a+2b-2}$$

is an appropriate choice.

Now we show that with this K we have $T_j^{(K)} = I$ for all $j = 1, \dots, p^b$. For this, it is in fact sufficient to show that this equality holds for all $j = 1, \dots, p^{b-1}$. Note that we already know that $T_{j_1}^{(K)} = T_{j_2}^{(K)}$ for $1 \le j_1 < j_2 \le p^b$. At this point we split our argument into two parts.

Assume first that $p = 2$. Let $(\alpha, \beta) \in T_1^{(K)}$. Then, choosing the j for which $\gamma_1(j) = 1$ in Lemma 3.3, by Lemma 3.1 we see that $(\alpha - 1, \beta) \in T_1^{(K)}$ is also valid (in view of $T_1^{(K)} = T_j^{(K)}$). This shows that for all $\alpha^* \in I_1$, we have $(\alpha^*, \beta) \in T_1^{(K)}$. Let now $(\hat\alpha, \hat\beta) \in I$ be arbitrary. Choose the j for which $\gamma_1(j)\beta \equiv \hat\beta \pmod{2^b}$. Then, since $(\hat\alpha + 1, \beta) \in T_1^{(K)}$, we obtain $(\hat\alpha, \hat\beta) \in T_1^{(K)}$. This proves our claim for $p = 2$.

Suppose next that p is an odd prime. Let $(\alpha, \beta) \in T_1^{(K)}$. Then, in view of $\gamma_{p-1}(p^{b-1}) \equiv -1 \pmod{p^b}$, applying Lemmas 3.1 and 3.3 with $t = p - 1$ and $j = p^b - 1$, we get that $(\alpha - p^a - 1, (-1)^{p^a+1}\beta) \in T_1^{(K)}$, that is, $(\alpha - 1, \beta) \in T_1^{(K)}$. This shows that in fact for all $\alpha^* \in I_1$, we have $(\alpha^*, \beta) \in T_1^{(K)}$. Let now $(\hat\alpha, \hat\beta) \in I$ be arbitrary. Based upon Lemma 3.3, choose $\gamma_{t_1}(j_1), \dots, \gamma_{t_\ell}(j_\ell) \in I_2$ in Lemma 3.3 such that $\gamma_{t_1}(j_1) \cdots \gamma_{t_\ell}(j_\ell)\beta \equiv \hat\beta \pmod{p^b}$. Then we inductively see that $(\alpha', \hat\beta) \in T_1^{(K)}$ with some $\alpha' \in I_1$. Indeed, we know that $(\alpha'', \gamma_{t_\ell}(j_\ell)\beta) \in T_{j'}^{(K+s)}$ for some s and j', but then this pair also belongs to $T_1^{(K)}$ - and so on. By what we have proved so far, this yields $(\hat\alpha, \hat\beta) \in T_1^{(K)}$. Thus our claim follows in this case, too.

So by Lemmas 3.1 and 3.3 we conclude that any interval of the form $[(j-1)p^{K-b+1}, jp^{K-b+1})$ $(j \ge 1)$ contains all elements of I. Thus the largest gap in $H^{(\alpha,\beta)}$ cannot be larger than $2p^{K-b+1}$ for any $(\alpha, \beta) \in I$. Hence the theorem follows. □

4. Acknowledgements

The authors are grateful to the referee for her/his useful and helpful remarks.

References

[1] D. Berend, *On the parity of exponents in the factorization of $n!$*, J. Number Theory **64** (1997), 13–19.

[2] D. Berend and G. Kolesnik, *Regularity of patterns in the factorization of $n!$*, J. Number Theory **124** (2007), 181–192.

[3] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.

[4] R. Breusch, *Zur Verallgemeinerung des Bertrandschen Postulates, das zwischen x und $2x$ stets Primzahlen liegen*, Math. Zeitschrift **34** (1932),

[5] U. Cerucci, F. Vaccarino, *Vector Linear Recurrence Sequences in Commutative Rings*, Applications of Fibonacci Numbers, 1996, pp. 63–72.

[6] Y.-G. Chen, *On the parity of exponents in the standard factorization of $n!$*, J. Number Theory **100** (2003), 326–331.

[7] Y.-G. Chen and Y.-C. Zhu, *On the prime power factorization of $n!$*, J. Number Theory **82** (2000), 1–11.

[8] J.-M. Deshouillers, F. Luca, *How often is $n!$ a sum of three squares?*, The Legacy of Alladi Ramakrishnan in the Mathematical Science, 2010, pp, 243–251.

[9] P. Erdős, *Über die Primzahlen gewisser arithmetischer Reihen*, Math. Zeitschrift **39** (1935), 473–491.

[10] P. Erdős and R. L. Graham, *Old and New Problems and Results in Combinatorial Number Theory*, L'Enseignement Mathématique, Imprimerie Kundig, Geneva, 1980.

[11] P. Erdős and R. Obláth, *Über diophantische Gleichungen der Form $n! = x^p \pm y^p$ und $n! \pm m! = x^p$*, Acta Litt. Sci. Szeged **8** (1937), 241–255.

[12] G. Everest, A. van der Poorten, I. Shparlinski, T. Ward, *Recurrence sequences*, Third Edition, American Matematical Society, 2015, pp. 318.

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

[14] R. K. Guy, *Unsolved Problems in Number Theory*, Third Edition, Springer, 2004.

[15] O. Klurman and M. Munsch, *Distribution of factorials modulo p*, J. Th. Nomb. Bordeaux **29** (2017), 169–177.

[16] E. Landau, *Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate*, Arch. Math. Phys. **13** (1908), 304–312.

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

[18] F. Luca and P. Stănică, *On the prime power factorization of $n!$*, J. Number Theory **102** (2003), 298–305.

[19] B. Rokowska and A. Schinzel, *Sur un problème de M. Erdős*, Elem. Mat. **15** (1960), 84–85.

[20] J. W. Sander, *On the Parity of Exponents in the Prime Factorization of Factorials*, J. Number Theory **90** (2001), 316–328.

[21] T. Shorey and R. Tijdeman, *Arithmetic Properties of Blocks of Consecutive Integers*, in: From Arithmetic to Zeta-Functions, Number Theory in Memory of Wolfgang Schwarz (J. Sander, J. Steuding, R. Steuding, eds), 2017, 455–471.

[22] S. S. Wagstaff, *The Schnirelmann density of the sums of three squares*, Proc. Amer. math. Soc. **52** (1975), 1–7.

L. Hajdu, Á. Papp
University of Debrecen, Institute of Mathematics
H-4010 Debrecen, P.O. Box 12.
Hungary
E-mail address: hajdul@science.unideb.hu
E-mail address: papp98@gmail.com