Available at WWW.MATHEMATICSWEB.ORG
POWERED BY SCIENCE @ DIRECT•

ACADEMIC PRESS

Journal of Number Theory 102 (2003) 298–305

JOURNAL OF Number Theory

http://www.elsevier.com/locate/jnt

On the prime power factorization of $n!$

Florian Luca[a] and Pantelimon Stănică[b,*,1]

[a] Instituto de Matematicas de lar UNAM, Campus Morelia, Apartado Postal 61-3 (Xangari) CP 58 089, Morelia, Michoacan, Mexico

[b] Department of Mathematics, Auburn University Montgomery, PO Box 244023, Montgomery, AL 36124-4023, USA

Received 20 September 2002; revised 25 March 2003

Communicated by D. Goss

Abstract

In this paper, we prove two results. The first theorem uses a paper of Kim (J. Number Theory 74 (1999) 307) to show that for fixed primes $p_1, \dots, p_k$, and for fixed integers $m_1, \dots, m_k$, with $p_i \nmid m_i$, the numbers $(e_{p_1}(n), \dots, e_{p_k}(n))$ are uniformly distributed modulo $(m_1, \dots, m_k)$, where $e_p(n)$ is the order of the prime p in the factorization of $n!$. That implies one of Sander's conjectures from Sander (J. Number Theory 90 (2001) 316) for any set of odd primes. Berend (J. Number Theory 64 (1997) 13) asks to find the fastest growing function $f(x)$ so that for large x and any given finite sequence $\varepsilon_i \in \{0, 1\}$, $i \leqslant f(x)$, there exists $n < x$ such that the congruences $e_{p_i}(n) \equiv \varepsilon_i \pmod 2$ hold for all $i \leqslant f(x)$. Here, p_i is the ith prime number. In our second result, we are able to show that $f(x)$ can be taken to be at least $c_1(\log x/(\log\log x)^6)^{1/9}$, with some absolute constant c_1, provided that only the first odd prime numbers are involved.

1. Introduction

For a prime number p and every positive integer m let $e_p(n)$ be the power at which the prime number p appears in the prime factorization of $n!$. In [6], it was asked whether for every fixed positive integer k there exists a positive integer n so that all the numbers $e_{p_i}(n)$ are even, where $p_1 < p_2 < \cdots < p_k$ denote the first k prime numbers. The above question was answered in the affirmative by Berend in [1]. In fact, Berend

*Corresponding author.
E-mail address: pstanica@mail.aum.edu (P. Stănică).
[1] Also associated with the Institute of Mathematics of Romanian Academy, Bucharest, Romania.

0022-314X/03/$ - see front matter © 2003 Elsevier Inc. All rights reserved.
doi:10.1016/S0022-314X(03)00102-1

proved more, namely that for a fixed value of $k \geqslant 1$ the number of positive integers satisfying the above property has bounded gaps. Specifically, there exists a computable constant $C(k)$, depending only on k, such that every interval of length $C(k)$ of positive numbers contains a positive integer n satisfying the above property. This result has been extended in [5] to the following setting: There exists a positive constant $C(k)$ depending only on k, such that if $\varepsilon_i \in \{0, 1\}$ (for $i = 1, \ldots, k$) are such that there exists at least one positive integer n satisfying the congruences $e_{p_i}(n) \equiv \varepsilon_i \pmod 2$ for all $i = 1, \ldots, k$, then there exist infinitely many such positive integers n, and the set of such positive integers has gaps bounded by $C(k)$. This extends the result of Berend on the original problem addressed by Erdős and Graham, because there $n = 1$ clearly satisfies the above congruences with $\varepsilon_i = 0$ for all $i = 1, \ldots, k$. The authors of [5] mention that for $2 \leqslant k \leqslant 5$ every pattern $\varepsilon_i \in \{0, 1\}$ for $1 \leqslant i \leqslant k$ appears at least once (hence, infinitely often by the above result), and they conjectured that every pattern of length k appears for all values of $k \geqslant 1$. This conjecture was recently proved by Chen [4]. In [9], a stronger conjecture is stated, and this conjecture was mentioned by Yong-Gao Chen in his talk at the ICM2002 in Beijing.

Conjecture 1 (Sander [9]). *Let $p_1, \ldots, p_k$ be distinct primes, and let $\varepsilon_1, \ldots, \varepsilon_k \in \{0, 1\}$. Then*

$$|\{0 \leqslant n < N : e_{p_i}(n) \equiv \varepsilon_i \pmod 2, \ \ 1 \leqslant i \leqslant k\}| \sim \frac{N}{2^k} \quad \text{as } N \to \infty.$$

In [9], it is shown that the above conjecture holds for $k = 1$, and it is also shown that every pattern of length 2 appears with two arbitrary primes p_1 and p_2.

In this paper, we first address the following more general conjecture:

Conjecture 2. *Let $p_1, \ldots, p_k$ be distinct primes, $m_1, \ldots, m_k$ be arbitrary positive integers ($\geqslant 2$), and $0 \leqslant a_i \leqslant m_i - 1$ for $i = 1, \ldots, k$ be arbitrary residue classes modulo m_i. Then*

$$|\{0 \leqslant n < N : e_{p_i}(n) \equiv a_i \pmod{m_i}, 1 \leqslant i \leqslant k\}| \sim \frac{N}{m_1 \ldots m_k} \quad \text{as } N \to \infty.$$

Thus, Conjecture 2 says that for fixed prime numbers $p_1, \ldots, p_k$ and for fixed integers $m_1, \ldots, m_k$ the numbers $(e_{p_1}(n), \ldots, e_{p_i}(n))$ should be uniformly distributed modulo $(m_1, \ldots, m_k)$, which is just a natural extension of Conjecture 1.

We give the following partial result which resolves the above Conjecture 2 under some technical assumptions.

Theorem 1. *Let $p_1, \ldots, p_k$ be distinct primes, $m_1, \ldots, m_k$ be arbitrary positive integers ($\geqslant 2$) and $0 \leqslant a_i \leqslant m_i - 1$ for $i = 1, \ldots, k$ be arbitrary residue classes modulo m_i. Assume further that $p_i \nmid m_i$ for $i = 1, \ldots, k$. Then*

$$|\{0 \leqslant n < N : e_{p_i}(n) \equiv a_i \pmod{m_i}, 1 \leqslant i \leqslant k\}| = \frac{N}{m_1 \ldots m_k} + O(N^{1-\delta}),$$

with $\delta := 1/(120k^2 p^{3m} m^2)$, where $m := \max\{m_i : 1 \leqslant i \leqslant k\}$, and $p := \max\{p_i : 1 \leqslant i \leqslant k\}$.

Notice that Theorem 1 not only proves Conjecture 2 under the particular assumptions that $p_i \nmid m_i$ for $i = 1, \ldots, k$, but it even gives an upper bound on the size of the error term. In particular, Theorem 1 proves Conjecture 1 for all finite sets of prime numbers not containing the prime number 2.

In the last section of his paper [1], Berend asks the following question: Assume that $2 = p_1 < p_2 < \cdots$ is the increasing sequence of all the prime numbers. Given $k \geqslant 1$ and an arbitrary pattern $\varepsilon_i \in \{0, 1\}$ for $i = 1, 2, \ldots, k$, how far does one need to go (as a function of k) in order to insure that one finds a number n so that $e_{p_i}(n) \equiv \varepsilon_i \pmod 2$. Since there are exactly 2^k such patterns, we expect such a number to be larger than 2^k. Put it differently, find the fastest growing function $f(x)$ such that for large x there exists $n < x$ such that the congruences $e_{p_i}(n) \equiv \varepsilon_i \pmod 2$ hold for all $i \leqslant f(x)$, where ε_i is an arbitrary function defined on the set of positive integers with values in $\{0, 1\}$. While we are unable to prove that $f(x)$ can be taken of the form $c \log x$ with some constant c (the optimal one being $1/\log 2$), we can give the following lower bound for $f(x)$.

Theorem 2. *Let $3 = p_1 < p_2 < \cdots$ be the sequence of odd prime numbers and let $(\varepsilon_i)_{i \geqslant 1}$ be an arbitrary sequence taking only the values 0 and 1. Then there exists an absolute constant c_1 such that for each large positive real number x, there exists a positive integer $n < x$ such that all congruences*

$$e_{p_i}(n) \equiv \varepsilon_i \pmod 2, \quad i = 1, \ldots, k(x)$$

hold with $k(x) := \left\lfloor c_1 \left(\frac{\log x}{(\log \log x)^6} \right)^{1/9} \right\rfloor$.

2. The proofs

In 1999, Kim (see [8]) published a very important paper in which he generalized results of Gelfond [7], Bésineau [2], and others, concerning the joint distribution of completely q-additive functions in residue classes. The results from Kim's paper found immediate applications, an example of such being a paper by Tichy and Thuswaldner (see [10]), in which these two authors use Kim's results to prove a version of the Erdős–Kac theorem for sets described by congruence properties of systems of completely q-additive functions.

In this paper, we point out that our theorems are immediate applications of Kim's main result.

We now describe Kim's main result, and explain how it can be used to prove our results.

Let $q \geqslant 2$ be any integer. A function f defined on $\mathbf{N} \cup \{0\}$ satisfying $f(0) = 0$ and $f(aq^k + b) = f(a) + f(b)$ for all integers $a \geqslant 1$, $k \geqslant 1$, and $0 \leqslant b < q^k$ is called *completely q-additive*. Note that a completely q-additive function may be characterized also as given by the sum of the values of some function, taken over the base q digits of the argument.

Let $\mathbf{q} := (q_1, \ldots, q_k)$, and $\mathbf{m} := (m_1, \ldots, m_k)$ be k-tuples of integers satisfying $q_i, m_i \geqslant 2$ for $i = 1, \ldots, k$, and $\gcd(q_i, q_j) = 1$ for $i \neq j$. For each i, let f_i be a completely q_i-additive function with integer values, and write $\mathbf{f} := (f_1, \ldots, f_k)$. Define

$$F_i := f_i(1), \tag{1}$$

$$d_i := \gcd(m_i, (q_i - 1)F_i, f_i(r) - rF_i \ (2 \leqslant r \leqslant q_i - 1)), \tag{2}$$

and let $\mathbf{F} := (F_1, \ldots, F_k)$ and $\mathbf{d} := (d_1, \ldots, d_k)$. For brevity, we write $\mathbf{f}(n) \equiv \mathbf{a} \pmod{\mathbf{m}}$ if the congruence $f_i(n) \equiv a_i \pmod{m_i}$ holds for all $i = 1, \ldots, k$. Assume further that $\gcd(F_i, d_i) = 1$ for all $i = 1, \ldots, k$, and that $\gcd(d_i, d_j) = 1$ for all $i \neq j$. Kim's theorem says the following:

Theorem K (Kim [8]). *With the previous assumptions and notations, the estimate*

$$|\{0 \leqslant n < N\colon \mathbf{f}(n) \equiv \mathbf{a} \pmod{\mathbf{m}}\}| = \frac{N}{m_1 \ldots m_k} + O(N^{1-\delta_1}) \tag{3}$$

holds as N goes to infinity, and for all k-tuples of residue classes $\mathbf{a}$ *modulo* $\mathbf{m}$, *where* $\delta_1 := 1/(120k^2q^3m^2)$, *with* $q := \max\{q_i\colon 1 \leqslant i \leqslant k\}$, *and* $m := \max\{m_i\colon 1 \leqslant i \leqslant k\}$.

Proof of Theorem 1. To apply Kim's theorem, let i be any fixed index in $\{1, \ldots, k\}$. Let λ_i be the minimal positive integer such that the congruence $\frac{p_i^{\lambda_i} - 1}{p_i - 1} \equiv 0 \pmod{m_i}$ holds. Such a value λ_i exists because $p_i \nmid m_i$. Clearly, $\lambda_i \geqslant 2$ because $m_i \geqslant 2$. To estimate λ_i from above, write $m_i := m_i' m_i''$, where m_i' and m_i'' are coprime, all the prime factors of m_i' divide $p_i - 1$, and m_i'' is coprime to $p_i - 1$. It is clear that m_i' and m_i'' are uniquely determined. By the well-known divisibility properties of Lucas sequences (see [3]), it follows easily that the number $\mu_i := m_i' \phi(m_i'')$ satisfies the condition that $\frac{p_i^{\mu_i} - 1}{p_i - 1} \equiv 0 \pmod{m_i}$. Here, for an arbitrary positive integer n we used $\phi(n)$ to denote the Euler ϕ function of n. It is easy to see that $m_i' \phi(m_i'') \geqslant 2$ holds for all positive integers $m_i \geqslant 2$ (if $m_i = 2$, then p_i is odd, in which case $\lambda_i = m_i' = m_i = 2$, while if $m_i > 2$, then either $m_i' \geqslant 2$, or $\phi(m_i'') = \phi(m_i) \geqslant 2$). In particular, $\lambda_i \leqslant m_i \leqslant m$, where the number m is defined in the statement of Theorem 1.

We now write $q_i := p_i^{\lambda_i}$. Notice that $\gcd(q_i, q_j) = 1$ holds for all $i \neq j$, and that $q := \max\{q_i\colon 1 \leqslant i \leqslant k\} \leqslant p^m$, where p and m are defined in the statement of Theorem 1.

Define the completely q_i-additive function f_i as follows. Let a be an integer in the interval $0 \leqslant a \leqslant q_i - 1$, and write it in base p_i as

$$a := a_0 + a_1 p_i + \cdots + a_{\lambda_i - 1} p_i^{\lambda_i - 1} \quad \text{with } 0 \leqslant a_j \leqslant p_i - 1 \text{ for } j = 0, \ldots, \lambda_i - 1. \tag{4}$$

Set

$$f_i(a) := a_0\frac{p_i^0 - 1}{p_i - 1} + a_1\frac{p_i - 1}{p_i - 1} + \cdots + a_{\lambda_i - 1}\frac{p_i^{\lambda_i - 1} - 1}{p_i - 1}, \tag{5}$$

and extend f_i in the obvious way to all the nonnegative integers in such a way that it becomes completely q_i-additive. A compact formula of f_i in all nonnegative integers is obtained as follows. Let $n \geqslant 0$, and write it in base p_i as

$$n := n_0 + n_1 p_i + \cdots + n_t p_i^t \quad \text{with } 0 \leqslant n_j \leqslant p_i - 1 \ \text{ for all } j = 0, \ldots, t. \tag{6}$$

For every nonnegative integer j write $\bar{j} \equiv j \pmod{\lambda_i}$ (the least residue). Then

$$f_i(n) = \sum_{j=0}^{t} n_j \frac{p_i^{\bar{j}} - 1}{p_i - 1}. \tag{7}$$

The next observation is that $f_i(n) \equiv e_{p_i}(n) \pmod{m_i}$. Indeed, it is well-known that, if the base p_i representation of n is given by (6), then

$$e_{p_i}(n) = \sum_{j=0}^{t} n_j \frac{p_i^{j} - 1}{p_i - 1}. \tag{8}$$

Thus, comparing (7) with (8), it suffices to show that

$$\frac{p_i^{j} - 1}{p_i - 1} \equiv \frac{p_i^{\bar{j}} - 1}{p_i - 1} \pmod{m_i},$$

which is equivalent to

$$\frac{p_i^{j - \bar{j}} - 1}{p_i - 1} \equiv 0 \pmod{m_i},$$

and the last congruence is obvious by the definition of λ_i and by the fact that $j - \bar{j}$ is a multiple of λ_i.

Having concluded that the completely q_i-additive function f_i represents precisely e_{p_i} modulo m_i, in order to complete the proof of Theorem 1, it suffices, via Theorem K, to verify that the functions f_i satisfy the assumptions of Theorem K. But it is clear that by choosing $r := p_i$, then $2 \leqslant r \leqslant q_i - 1$ (because $\lambda_i \geqslant 2$), and with such an r we have $f_i(r) - rF_i = f_i(p_i) = 1$ (notice that $F_i = f_i(1) = 0$). Thus, formula (2) tells us that $d_i = 1$, therefore that all the relations $\gcd(F_i, d_i) = 1$ for $i = 1, \ldots, k$, and $\gcd(d_i, d_j) = 1$ for $i \neq j$ hold. All the assertions of Theorem 1 can now be read off from Theorem K. □

Proof of Theorem 2. Given k, we shall apply Kim's theorem with the error term to find $N := N(k)$ in such a way as to make sure that there exists $n < N$ such that $e_{p_i}(n) \equiv \varepsilon_i \pmod 2$. In order to do so, we shall need first to find the dependence of the constants understood in O from Theorem K as a function of the data k, m, and q. A close analysis of Kim's arguments points out that the error term appearing in Theorem K can be made explicit by going through the arguments from Propositions 1 and 2 in [8]. In both Propositions 1 and 2 in [8], the constant understood in the error term can be taken to be of the type $c_2 k^{1/2} q$, where c_2 is an absolute constant. Thus, with Theorem 1, we have that $m := 2$, p_k is the kth odd prime, $q := p_k^2$, and $\delta := 1/(480k^2 p_k^6)$. By Theorem 1 and Kim's theorem with the explicit dependence of O on the initial data, it follows that there exists an absolute constant c_3 such that whenever the inequality

$$\frac{N}{2^k} > c_3 k^{1/2} p_k^2 N^{1-\delta} \tag{9}$$

holds, then there must exist a positive integer $n < N$ such that $e_{p_i}(n) \equiv \varepsilon_i \pmod 2$ holds for all $i = 1, 2, \ldots, k$. Inequality (9) is equivalent to

$$\log N > \frac{1}{\delta} \log(c_3 2^k k^{1/2} p_k^2) = 480k^2 p_k^6 (\log c_3 + k \log 2 + 0.5 \log k + 2 \log p_k). \tag{10}$$

With the Prime Number Theorem, we have $p_k = (1 + o(1))k \log k$, and so inequality (10) yields

$$\log N > 480(\log 2)(1 + o(1))k^9 \log^6 k. \tag{11}$$

Setting $x := N$ in the left-hand side of the above inequality, and expressing k as a function of x, we see that there exists indeed an absolute constant c_1 so that by setting k to be the largest integer less than or equal to $c_1 \left(\frac{\log x}{(\log \log x)^6}\right)^{1/9}$ then inequality (11) holds. □

3. Comments

In this note, we just pointed out how problems about the distributions of exponents of (fixed) primes appearing in the prime power factorization of $n!$ in residue classes should be tackled via the general theory of joint distributions of completely q-additive functions in residue classes. Indeed, by the simple observation of treating this problem in this way, we pointed out that a result far more general than any other results available in the literature on this topic can be inferred in a straightforward way from Kim's results. In this spirit, we assert that it is probably not too hard to prove Conjecture 2 in its full generality. However, in order to do so, it is probably far more interesting and worthwhile to try to prove an extension of Kim's results to the following setting.

Let $\mathbf{q} := (q_1, \ldots, q_k)$, $\mathbf{m} := (m_1, \ldots, m_k)$, and $\mathbf{f} := (f_1, \ldots, f_k)$ be as in Kim's theorem. Let further $\mathbf{u} := (u_1, \ldots, u_k)$ and $\mathbf{v} := (v_1, \ldots, v_k)$, where $u_i \geqslant 1$ and v_i are nonnegative integers for $i = 1, \ldots, k$. Write $\mathbf{f}(\mathbf{u}n + \mathbf{v}) = (f_1(u_1 n + v_1), \ldots, f_k(u_k n +$

$v_k)$). We argue that it would be worthwhile to study the distribution of the positive integers n such that $\mathbf{f}(\mathbf{u}n+\mathbf{v}) \equiv \mathbf{a} \pmod{\mathbf{m}}$, and to conclude that, under certain natural arithmetical conditions on $\mathbf{q}, \mathbf{m}, \mathbf{u}, \mathbf{v}$ and $\mathbf{f}$, the numbers $\mathbf{f}(\mathbf{u}n+\mathbf{v})$ are uniformly distributed in arithmetical progressions. For example, let us see how one would attempt to include the number 2 into the picture in order to prove Conjecture 1 in its full generality. If p_i is an odd prime, then define the completely q_i-additive function f_i as in the present paper. When $p_i = 2$, then if one writes n binary as $n := n_0 + 2n_1 + \cdots + 2^t n_t$, with $n_i \in \{0, 1\}$ for $i = 0, \ldots, t$, then $e_{p_i}(n) \equiv n_1 + \cdots + n_t \pmod 2$. Fix $\varepsilon_i \in \{0, 1\}$, and assume that $p_1 = 2$. For $i = 1$, define $f_1(n)$ to be the sum of the digits of n in base 2. Consider the system of congruences:

$$f_i(2n) \equiv \varepsilon_i \quad \text{for } i = 1, \ldots, k \tag{12}$$

and

$$f_1(2n+1) \equiv \varepsilon_1 + 1, \quad f_i(2n+1) \equiv \varepsilon_i \qquad \text{for } i = 2, \ldots, k. \tag{13}$$

If Kim's theorem could be extended as we pointed out above under pertinent assumptions on $\mathbf{q}, \mathbf{m}, \mathbf{u}, \mathbf{v}$ and $\mathbf{f}$, and if such pertinent assumptions were fulfilled for the systems of congruences (12) and (13), (with the obvious choices on $\mathbf{q}, \mathbf{m}, \mathbf{u}, \mathbf{v}$ and $\mathbf{f}$), then one would get a positive answer to Conjecture 1. By a procedure similar to the one indicated above, one could also get a positive answer to Conjecture 2 via such an extension of Kim's results.

Acknowledgments

We thank Jean-Marie De Koninck and the referee for suggestions which improved the presentation of this paper. The first author was supported in part by Grants SEP-CONACYT 37259-E and 37260-E. The second author was partially supported by a research grant from the School of Sciences at his institution.

References

[1] D. Berend, On the parity of exponents in the factorization of $n!$, J. Number Theory 64 (1997) 13–19.
[2] J. Bésineau, Indépendance statistique d'ensembles liés à la fonction "somme des chiffres", Acta Arith. 20 (1972) 401–416.
[3] Y. Bilu, G. Hanrot, P.M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, With an appendix by M. Mignotte, J. Reine Angew. Math. 539 (2001) 75–122.
[4] Y.-G. Chen, On the parity of exponents in the standard factorization of $n!$, J. Number Theory 100 (2003) 326–331.
[5] Y.-G. Chen, Y.-C. Zhu, On the prime power factorization of $n!$, J. Number Theory 82 (2000) 1–11.
[6] P. Erdős, R.L. Graham, Old and New Problems and Results in Combinatorial Number Theory, L'Enseignement Mathématique, Imprimerie Kundig, Geneva, 1980.
[7] A.O. Gelfond, Sur les nombres qui ont des propriétés additives et multiplicatives données, Acta Arith. 13 (1968) 259–265.

[8] D.-H. Kim, On the joint distribution of q-additive functions in residue classes, J. Number Theory 74 (1999) 307–336.
[9] J.W. Sander, On the parity of exponents in the prime factorization of factorials, J. Number Theory 90 (2001) 316–328.
[10] R.F. Tichy, J.M. Thuswaldner, An Erdős–Kac theorem for systems of q-additive functions, Indag. Math. 11 (2000) 283–291.