BULL. AUSTRAL. MATH. SOC. 11N25, 11B50
VOL. 73 (2006) [329–334]

ON THE EXPONENTS MODULO 3 IN THE STANDARD FACTORISATION OF $n!$

WEI LIU AND YONG-GAO CHEN

Let p be a prime and m be a positive integer. For a positive integer n, let $e_p(n)$ be the nonnegative integer with $p^{e_p(n)} \mid n$ and $p^{e_p(n)+1} \nmid n$. As a corollary of our main result we derive an asymptotic formula for the counting function with regard to the condition $e_p(n!) \equiv \varepsilon \pmod 3$, where $\varepsilon \in \mathbf{Z}_3$. In 2001, Sander proved the result with modulus 2.

1. INTRODUCTION

Let $p_1, p_2, \ldots$ be the sequence of all primes in ascending order. For a positive integer n, let $e_{p_i}(n)$ be the nonnegative integer with $p_i^{e_{p_i}(n)} \mid n$ and $p_i^{e_{p_i}(n)+1} \nmid n$. In 1997, Berend [1] proved a conjecture of Erdős and Graham (see [4, p. 77]) by showing that for every positive integer k there exist infinitely many positive integers n with

$$e_{p_1}(n!) \equiv 0 \pmod 2, e_{p_2}(n!) \equiv 0 \pmod 2, \ldots, e_{p_k}(n!) \equiv 0 \pmod 2,$$

where the differences between adjacent such n are less than effectively computable constant depending only on k. The initial case $n = 1$ is very useful in Berend's proof.

In 1999, Chen and Zhu [3] considered a general case. Two years later, Sander [6] posed two conjectures and proved some special cases of his conjectures. After Sander, Chen [2] proved one of the two conjectures posed by Sander: for any given positive integer k and any $\varepsilon_i \in \{0, 1\} (i = 1, 2, \ldots, k)$, there exist infinitely many positive integers n such that

$$e_{p_1}(n!) \equiv \varepsilon_1 \pmod 2, e_{p_2}(n!) \equiv \varepsilon_2 \pmod 2, \ldots, e_{p_k}(n!) \equiv \varepsilon_k \pmod 2.$$

In 2003, F. Luca and P. Stănică [5] posed the following conjecture:

CONJECTURE (F.Luca and P.Stănică [5]). 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 class modulo m_i. Then

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

Received 10th October, 2005
The author was supported by the National Natural Science Foundation of China, Grant No 10471064. The authors would like to thank the referee for his/her useful comments.

In their paper, they proved the conjecture under the assumption that $p_i \nmid m_i (i = 1, \dots, k)$.

Sander [6] derived an asymptotic formula for the proportion of $n < N$ for which $e_p(n!) \equiv \varepsilon \pmod 2$. In the present paper, we improve the method in Sander [6] and derive an asymptotic formula for the counting function with regard to the condition $e_p(n!) \equiv \varepsilon \pmod 3$, where p is a prime and $\varepsilon \in \mathbf{Z}_3$. At the same time we prove a more general result. Although it is also a special case of Luca-Stănică Conjecture, the following theorem not only gives a good bound for the error term, but also can take any prime p as modulus.

Let m be a fixed positive integer. For $\varepsilon \in \mathbf{Z}_m$ and a prime p, let

$$E_{p,\,\varepsilon,\,m}(N) := \Big|\{0 \leqslant n < N : e_p(n!) \equiv \varepsilon \pmod m\}\Big|.$$

THEOREM. *For any prime p with $p \equiv \pm 1 \pmod m$ or $p \equiv 0 \pmod m$ and any $\varepsilon \in \mathbf{Z}_m$, we have*

$$E_{p,\,\varepsilon,\,m}(N) = \frac{1}{m}N + O(N^{1/2}).$$

REMARK. From the proof of the theorem, we can see that

$$\Big|E_{p,\,\varepsilon,\,m}(N) - \frac{1}{m}N\Big| \leqslant 4p^{3/2}N^{1/2}.$$

Noting that all primes have the property that $p \equiv \pm 1 \pmod 3$ or $p \equiv 0 \pmod 3$, by the theorem, we get the following corollary:

COROLLARY 1. *For any prime p and any $\varepsilon \in \mathbf{Z}_3$, we have*

$$E_{p,\,\varepsilon,\,3}(N) = \frac{1}{3}N + O(N^{1/2}).$$

By setting $m = p$ in the theorem we get the corollary:

COROLLARY 2. *Let p be a prime. For any $\varepsilon \in \mathbf{Z}_p$, we have*

$$E_{p,\,\varepsilon,\,p}(N) = \frac{1}{p}N + O(N^{1/2}).$$

2. Proof of the theorem

Let p be a prime, m be a positive integer and let the nonnegative integer n have the p-adic expansion $n = n_s p^s + \cdots + n_1 p + n_0$ with p-adic digits $0 \leqslant n_j < p$ for $0 \leqslant j \leqslant s$. It is well known that

$$e_p(n!) = \sum_{j=1}^{\infty}\Big[\frac{n}{p^j}\Big].$$

https://doi.org/10.1017/S000497270003536X Published online by Cambridge University Press

Hence,

$$e_p(n!) = \sum_{j=1}^{s} n_j(p^{j-1} + \cdots + p + 1) \equiv \sum_{j=1}^{s} a_j n_j \pmod{m},$$

where $a_j \equiv p^{j-1} + \cdots + p + 1 \pmod{m}$ and $0 \leqslant a_j < m, j = 1, \ldots, s$. Now, we give two lemmas first.

Lemma 1. *Let p be a prime, m be a positive integer, and $r \geqslant 2$ be an integer. For a fixed integer k $(1 \leqslant k \leqslant m-1)$, we have*

$$\left|\{j \mid 1 \leqslant j \leqslant r-1 \text{ and } ka_j \equiv 0 \pmod{m}\}\right| \leqslant \frac{r-1}{2},$$

where $a_j (j = 1, \ldots, r-1)$ are defined as above.

Proof: Suppose that $m \mid ka_j$ and $m \mid ka_{j+1}$ for some $j (1 \leqslant j \leqslant r-2)$. By the definition of $a_j (1 \leqslant j \leqslant r-1)$, we have $m \mid kp^j$.

Assume that $m = p^\alpha m_1$, where $p \nmid m_1$ and $\alpha \geqslant 0$. Since $m \mid ka_j$, we have $m \mid k(1+p+\cdots+p^{j-1})$. Hence, $p^\alpha \mid k(1+p+\cdots+p^{j-1})$. Since $(p, 1+p+\cdots+p^{j-1}) = 1$, we have $p^\alpha \mid k$. Then assume that $k = k_1 p^\alpha$, where k_1 be an integer. From $m \mid kp^j$, we have that $kp^j = k_1 p^{\alpha+j} \equiv 0 \pmod{m}$, hence, $m_1 \mid k_1$. Now, we have $m \mid k$, a contradiction with $1 \leqslant k \leqslant m-1$.

Hence, for each $j (j = 1, \ldots, r-2)$, we have either $ka_j \not\equiv 0 \pmod{m}$ or $ka_{j+1} \not\equiv 0 \pmod{m}$.

By $ka_1 = k \not\equiv 0 \pmod{m}$, we obtain a proof of Lemma 1. ∎

Lemma 2. *Let p be a prime, m be a positive integer, $r \geqslant 0$, $U \geqslant 1$ and $T \geqslant 0$ be integers with $U \equiv \pm 1 \pmod{m}$ or $U \equiv 0 \pmod{m}$, and let $\varepsilon \in \{0, 1, \ldots, m-1\}$. Then*

$$C(\varepsilon) := \left|\left\{(n_r, \ldots, n_0) \in \mathbb{Z}^{r+1} : 0 \leqslant n_j < U (0 \leqslant j < r); 0 \leqslant n_r < T; \sum_{j=1}^{r} a_j n_j \equiv \varepsilon \pmod{m}\right\}\right|,$$

where a_j $(j = 1, \ldots, r)$ are defined as above and $\sum_{j=1}^{r} a_j n_j = 0$ for $r = 0$, satisfies

$$\left|C(\varepsilon) - \frac{1}{m} T U^r\right| \leqslant T U^{(r+1)/2}.$$

Proof: The result is trivial for $r = 0, 1$. Now we assume that $r \geqslant 2$. Let $\omega_k = e^{(2\pi i k)/m} (k = 0, 1, \ldots, m-1)$, which are all the roots of $x^m = 1$. Then for any integer $k (0 \leqslant k \leqslant m-1)$, we have

$$\begin{aligned} C(0) + \omega_k C(1) + \omega_k^2 C(2) + \cdots + \omega_k^{m-1} C(m-1) &= \sum_{n_0=0}^{U-1} \sum_{n_1=0}^{U-1} \cdots \sum_{n_{r-1}=0}^{U-1} \sum_{n_r=0}^{T-1} \omega_k^{\sum_{j=1}^{r} a_j n_j} \\ &= U \prod_{j=1}^{r-1} \Big(\sum_{n_j=0}^{U-1} \omega_k^{a_j n_j}\Big) \sum_{n_r=0}^{T-1} \omega_k^{a_r n_r}. \end{aligned}$$

https://doi.org/10.1017/S000497270003536X Published online by Cambridge University Press

Let $B(\varepsilon) = C(\varepsilon) - (1/m)TU^r$ $(0 \leqslant \varepsilon < m)$, we have

$$\begin{aligned} &B(0) + \omega_0 B(1) + \omega_0^2 B(2) + \cdots + \omega_0^{m-1} B(m-1) = 0, \\ &B(0) + \omega_k B(1) + \omega_k^2 B(2) + \cdots + \omega_k^{m-1} B(m-1) \\ &\qquad\qquad = U \prod_{j=1}^{r-1} \Big(\sum_{n_j=0}^{U-1} \omega_k^{a_j n_j} \Big) \sum_{n_r=0}^{T-1} \omega_k^{a_r n_r}, 1 \leqslant k \leqslant m-1. \end{aligned}$$

For any integer $u (1 \leqslant u \leqslant m)$, multiply both sides by ω_k^u, then add all the equations, we have

$$mB(m-u) = \sum_{k=1}^{m-1} \omega_k^u U \prod_{j=1}^{r-1} \Big(\sum_{n_j=0}^{U-1} \omega_k^{a_j n_j} \Big) \sum_{n_r=0}^{T-1} \omega_k^{a_r n_r}.$$

For a fixed $k (1 \leqslant k \leqslant m-1)$, it follows from Lemma 1 that

$$\big| \{ j \mid 1 \leqslant j \leqslant r-1 \ \text{ and } \ k a_j \equiv 0 \pmod{m} \} \big| \leqslant \frac{r-1}{2}.$$

If $k a_j \not\equiv 0 \pmod{m}$, since $U \equiv \pm 1 \pmod{m}$ or $U \equiv 0 \pmod{m}$, we have

$$\Big| \sum_{n_j=0}^{U-1} \omega_k^{a_j n_j} \Big| \leqslant 1.$$

Then

$$m \big| B(m-u) \big| \leqslant \sum_{k=1}^{m-1} T U^{(r-1)/2+1} \leqslant m T U^{(r+1)/2},$$

hence,

$$\big| B(m-u) \big| \leqslant T U^{(r+1)/2}.$$

Thus for any $\varepsilon (\varepsilon = 0, 1, \ldots, m-1)$, we have

$$\Big| C(\varepsilon) - \frac{1}{m} T U^r \Big| \leqslant T U^{(r+1)/2}.$$

This completes the proof of Lemma 2. ∎

PROOF OF THE THEOREM: We define $E_{p,\,\varepsilon,\,m}(L, M) := E_{p,\,\varepsilon,\,m}(L) - E_{p,\,\varepsilon,\,m}(M)$ for integers $L \geqslant M \geqslant 0$. Let $N = N_s p^s + \cdots + N_1 p + N_0$ be the p-adic expansion of N. Originating from the disjoint union of the corresponding sets, we immediately have

$$E_{p,\,\varepsilon,\,m}(N) = \sum_{k=0}^{s} E_{p,\,\varepsilon,\,m}(N_s p^s + \cdots + N_{s-k} p^{s-k}, N_s p^s + \cdots + N_{s-k+1} p^{s-k+1}),$$

where the empty sum occurring for $k = 0$ is considered to be 0.

https://doi.org/10.1017/S000497270003536X Published online by Cambridge University Press

For a fixed integer k, we obtain

$$
\begin{aligned}
&E_{p,\,\varepsilon,\,m}(N_sp^s+\cdots+N_{s-k}p^{s-k}, N_sp^s+\cdots+N_{s-k+1}p^{s-k+1}) \\
&\quad = \Bigl|\{n = N_sp^s+\cdots+N_{s-k+1}p^{s-k+1}+n_{s-k}p^{s-k}+\cdots+n_1p+n_0 : \\
&\qquad 0\leqslant n_{s-k-j}<p(1\leqslant j\leqslant s-k); 0\leqslant n_{s-k}<N_{s-k}; e_p(n!)\equiv\varepsilon \pmod m\}\Bigr| \\
&\quad = \biggl|\biggl\{(n_{s-k},\dots,n_0) : 0\leqslant n_j<p\ (0\leqslant j<s-k);\ 0\leqslant n_{s-k}<N_{s-k}; \\
&\qquad\qquad \sum_{j=1}^{s-k} a_jn_j \equiv \varepsilon - \sum_{j>s-k} a_jN_j \pmod m\biggr\}\biggr|.
\end{aligned}
$$

It follows from Lemma 2, that

$$
\Bigl|E_{p,\,\varepsilon,\,m}(N_sp^s+\cdots+N_{s-k}p^{s-k}, N_sp^s+\cdots+N_{s-k+1}p^{s-k+1}) - \frac{1}{m}N_{s-k}p^{s-k}\Bigr| \leqslant N_{s-k}p^{(s-k+1)/2}.
$$

Hence, we have

$$
\begin{aligned}
&\Bigl|E_{p,\,\varepsilon,\,m}(N) - \frac{1}{m}N\Bigr| \\
&\quad\leqslant \sum_{k=0}^{s}\Bigl|E_{p,\,\varepsilon,\,m}(N_sp^s+\cdots+N_{s-k}p^{s-k}, N_sp^s+\cdots+N_{s-k+1}p^{s-k+1}) - \frac{1}{m}N_{s-k}p^{s-k}\Bigr| \\
&\quad\leqslant \sum_{k=0}^{s} N_{s-k}p^{(s-k+1)/2}.
\end{aligned}
$$

Since $N_{s-k}<p$, $p\geqslant 2$ and $p^s\leqslant N$, we have

$$
\sum_{k=0}^{s} N_{s-k}p^{(s-k+1)/2} = \sum_{k=0}^{s} p^{(s-k+3)/2} = p^{(s+3)/2}\sum_{k=0}^{s} p^{-(k/2)} \leqslant 4p^{3/2}N^{1/2}.
$$

From it, we have $E_{p,\,\varepsilon,\,m}(N) = (1/m)N + O(N^{1/2})$. This completes the proof of the theorem. ∎

References

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

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

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

[4] P. Erdős and R.L. Graham, *Old and new problems and results in combinatorial number theory* (L'Enseignement Mathématique, Imprimerie Kundig, Geneva, 1980).

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

[6] J.W. Sander, 'On the parity of exponents in the prime factorization of factorials', *J. Number Theory* **90** (2001), 316–328.

Department of Mathematics
Nanjing Normal University
Nanjing 210097
China
e-mail:ygchen@njnu.edu.cn