# On the least common multiple of several random integers

Alin Bostan, Alexander Marynych, Kilian Raschel

# ON THE LEAST COMMON MULTIPLE OF SEVERAL RANDOM INTEGERS

ALIN BOSTAN, ALEXANDER MARYNYCH, AND KILIAN RASCHEL

Abstract. Let $L_n(k)$ denote the least common multiple of $k$ independent random integers uniformly chosen in $\{1, 2, \ldots, n\}$. In this note, using a purely probabilistic approach, we derive a criterion for the convergence in distribution as $n \to \infty$ of $\frac{f(L_n(k))}{n^{rk}}$ for a wide class of multiplicative arithmetic functions $f$ with polynomial growth $r > -1$. Furthermore, we identify the limit as an infinite product of independent random variables indexed by prime numbers. Along the way, we compute the generating function of a trimmed sum of independent geometric laws, occurring in the above infinite product. This generating function is rational; we relate it to the generating function of a certain max-type Diophantine equation, of which we solve a generalized version. Our results extend theorems by Erdős and Wintner (1939), Fernández and Fernández (2013) and Hilberdink and Tóth (2016).

## 1. Introduction

A celebrated result due to Dirichlet [13] states that two random positive integers are coprime with probability $6/\pi^2 \approx 0.61$. A heuristic argument goes as follows. A prime $p$ divides a random integer $X$ with probability $1/p$, and does not divide independent $X_1$ and $X_2$ simultaneously with probability $1 - 1/p^2$. Hence the event $\gcd(X_1, X_2) = 1$ occurs with probability

$$\prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p^2}\right) = \left(\sum_{n \geqslant 1} \frac{1}{n^2}\right)^{-1} = \frac{6}{\pi^2},$$

where $\mathcal{P} = \{2, 3, 5, \ldots\}$ denotes the set of prime numbers. An equivalent restatement is that two random positive integers admit an expected number of $\pi^2/6 \approx 1.64$ common positive integer divisors, or that the expected number of integers between 1 and $N$ which are coprime with $N$ equals $6N/\pi^2 \approx 0.61N$. More generally, Cesàro showed [7, 8] that for $k \geqslant 2$ positive random integers, the probability that they are relatively prime is $1/\zeta(k)$, where $\zeta(s) = \sum_{n \geqslant 1} n^{-s}$ is the Riemann zeta function. For a nice account of the rich history of Dirichlet's result, see [1].

As stated, these facts are however not very precise, since there is no uniform distribution on the set of positive integers. What we have implicitly considered above is the uniform distribution on $\{1, 2, \ldots, n\}$ and then we have taken the limit as $n$ goes to infinity. Formally, if $P_k(n)$ denotes the probability that $k$ positive

2010 *Mathematics Subject Classification.* Primary: 11A05, 11N37; Secondary: 11A25, 60F05.

*Key words and phrases.* Convergence in distribution, least common multiple, prime products, trimmed sums of geometric laws.

This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 759702.

integers, chosen uniformly at random from $\{1, 2, \ldots, n\}$, are relatively prime, then $P_k(n) = 1/\zeta(k) + O(1/n)$ for $k \geqslant 3$, and $P_2(n) = 1/\zeta(2) + O(\log n/n)$, and therefore $\lim_{n\to\infty} P_k(n) = 1/\zeta(k)$, see e.g. [25] and [12].

Cesàro also considered similar questions when the greatest common divisor (gcd) is replaced by the least common multiple (lcm). He proved in [9] that the expected lcm of two random integers is asymptotically equal to their product multiplied by the constant $\zeta(3)/\zeta(2) \approx 0.73$, and more generally that if $X_1^{(n)}$ and $X_2^{(n)}$ are independent copies of a random variable with the uniform distribution on $\{1, 2, \ldots, n\}$, then the moments $\mathbb{E}\{\mathrm{lcm}(X_1^{(n)}, X_2^{(n)})^r\}$ of their least common multiple behave like

$$\begin{aligned}\mathbb{E}\{\mathrm{lcm}(X_1^{(n)}, X_2^{(n)})^r\} \ &\sim \ \zeta(r+2)/\zeta(2) \cdot (\mathbb{E}(X_1^{(n)})^r)^2 \\ &\sim \ \frac{\zeta(r+2)}{\zeta(2)(r+1)^2} \cdot n^{2r}, \quad n \to \infty.\end{aligned}$$

In contrast with the case of the gcd, the extension of this result to the lcm of several random integers is much more subtle. This is the topic of the current note.

Let thus $X_1^{(n)}, X_2^{(n)}, \ldots, X_k^{(n)}$ be independent copies of a random variable $X^{(n)}$ with the uniform distribution on $\{1, 2, \ldots, n\}$. In what follows, we are interested in asymptotic properties of the distribution of the least common multiple

$$L_n(k) = \mathrm{lcm}\left(X_1^{(n)}, X_2^{(n)}, \ldots, X_k^{(n)}\right),$$

as $n \to \infty$, and more generally of the quantity $f(L_n(k))$, for a wide class of multiplicative arithmetic functions $f : \mathbb{N} \to \mathbb{C}$, with $\mathbb{N}$ denoting $\{1, 2, 3, \ldots\}$. Recall that a function $f$ is said to be *arithmetic* if its domain of definition is $\mathbb{N}$ and its range is $\mathbb{C}$. An arithmetic function is called *multiplicative* if $f(1) = 1$ and if $f(mn) = f(m)f(n)$ as soon as $m$ and $n$ are coprime.

Our motivation for the present paper comes from two recent works, one by Fernández and Fernández [18] and the other by Hilberdink and Tóth [22].

In 2013 Fernández and Fernández proved, see Theorem 3(b) in [18], a generalization of Cesàro's result for the lcm of three random integers. More precisely, they showed that the moments $\mathbb{E}\{(L_n(3))^r\}$ behave asymptotically like $\frac{C_{r,3}}{(r+1)^3} \cdot n^{3r}$ as $n$ tends to infinity for every fixed $r \in \mathbb{N}$. Here, the constant $C_{r,3}$ is equal (in the notation of [18]) to $C_{r,3} = T_3\zeta(2r+3)J(r+2)$, where $T_3 = \prod_{p\in\mathcal{P}}(1-1/p)^2(1+2/p)$ is the asymptotic proportion of triples of integers that are pairwise coprime, and where $J(r+2)$ is the Dirichlet series $J(r+2) = \prod_{p\in\mathcal{P}}\left(1 + \frac{3(p+1)}{(p+2)(p^{r+2}-1)}\right)$. An easy computation shows that the constant $C_{r,3}$ admits the equivalent expression

$$C_{r,3} = \zeta(r+2)\zeta(2r+3)\prod_{p\in\mathcal{P}}\left(1-\frac{1}{p}\right)^2\left(1+\frac{2}{p}+\frac{2}{p^{r+2}}+\frac{1}{p^{r+3}}\right). \tag{1}$$

In particular the expected lcm of three random positive integers is asymptotically equal to their product multiplied by the constant $C_{1,3} \approx 0.34$. The method used by Fernández and Fernández [18, §4] relies on probabilistic arguments combined with the classical identity

$$\mathrm{lcm}(X_1, X_2, X_3) = \frac{X_1X_2X_3\mathrm{gcd}(X_1, X_2, X_3)}{\mathrm{gcd}(X_1, X_2)\mathrm{gcd}(X_2, X_3)\mathrm{gcd}(X_3, X_1)}.$$

Although this identity does admit a generalization for $k > 3$ integers, the probabilistic arguments used in [18] do not seem to extend smoothly to the case $k > 3$.

Instead of that, for arbitrary $k \in \mathbb{N}$, Fernández and Fernández provide in Theorem 1 in [18] upper (resp. lower) bounds for the upper (resp. lower) limit of the probability $\mathbb{P}\{L_n(k) \leqslant xn^k\}$, $x \in (0,1)$, but these upper and lower bounds are different. Only for $k = 2$ and $k = 3$ these bounds imply that the sequence $(\mathbb{E}\{(L_n(k)/n^k)^r\})_{n\in\mathbb{N}}$ actually converges to a nondegenerate limit, which is $(r+1)^{-2}\zeta(r+2)/\zeta(2)$ when $k = 2$ and the aforementioned constant $(r+1)^{-3}C_{r,3}$ when $k = 3$.

It is natural to ask whether such a convergence result also holds for $k > 3$. The *positive* answer to this question is implicit in the work of Hilberdink and Tóth [22], see Theorem 2.1 therein. Generalizing both the results of Cesàro [9] (for $k = 2$) and Fernández and Fernández [18] (for $k = 3$), they managed to prove that for any $k \geqslant 2$ and $r \in \mathbb{N}$, the moments $\mathbb{E}\{(L_n(k))^r\}$ behave asymptotically like $(r+1)^{-k}C_{r,k} \cdot n^{kr}$ as $n$ tends to infinity, where the constant $C_{r,k}$ is equal to

$$C_{r,k} = \prod_{p\in\mathcal{P}} \left(1 - \frac{1}{p}\right)^k \sum_{\ell_1,\ldots,\ell_k=0}^{\infty} \frac{p^{r\,\max(\ell_1,\ldots,\ell_k)}}{p^{(r+1)(\ell_1+\cdots+\ell_k)}}. \tag{2}$$

Hilberdink and Tóth also proved, see Corollary 1 in [22], that the $k$-variate sum above simplifies in the cases $k = 2$, $k = 3$ and $k = 4$ to an explicit rational function in $1/p$, allowing to retrieve the value $C_{r,2} = \zeta(r+2)/\zeta(2)$ due to Cesàro, and the value $C_{r,3}$ in Eq. (1) due to Fernández and Fernández. The method used by Hilberdink and Tóth for $k \in \{2,3,4\}$ is effective and could yield an algorithm that computes (in principle) a formula similar to (1) for any given $k$. However, the algorithm has complexity exponential in $k$, so in practice it yields formulas for few values of $k$.

One of the byproducts of the present work is that we further simplify the expression of $C_{r,k}$ in (2). Precisely, we prove, see Corollary 2.7 below, that

$$C_{r,k} = \prod_{p\in\mathcal{P}} F_{r,k}\left(\frac{1}{p}\right), \quad k, r \in \mathbb{N}.$$

where $F_{r,k}(x)$ is the following *explicit univariate* rational function:

$$F_{r,k}(x) = \left(\frac{1-x}{1-x^{r+1}}\right)^k \cdot \sum_{j=1}^{k} \binom{k}{j} (-1)^{j-1} \frac{1-x^{j(r+1)}}{1-x^{(j-1)(r+1)+1}}, \quad k, r \in \mathbb{N}, \quad |x| < 1.$$

The fact that the term in the product defining $C_{r,k}$ in (2) is a rational function in $1/p$ is not surprising. This follows from the fact that if $\alpha_{r,k,\ell}$ denotes the number of solutions in $\mathbb{N}_0^k$, where $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, of the max-type linear Diophantine equation

$$(r+1)(\ell_1 + \cdots + \ell_k) - r\,\max(\ell_1, \ldots, \ell_k) = \ell, \quad k, r \in \mathbb{N}, \quad \ell \in \mathbb{N}_0, \tag{3}$$

then a classical result due to Ehrhart [14] implies that the generating functions

$$x \mapsto \sum_{\ell=0}^{\infty} \alpha_{r,k,\ell} x^\ell$$

are rational. Indeed, one can split the orthant $\mathbb{N}_0^k$ into wedges $x_{\sigma(1)} \geqslant \cdots \geqslant x_{\sigma(k)}$, where $\sigma$ is a permutation of $\{1, \ldots, k\}$, get a rational generating function on each wedge by [14], and use inclusion-exclusion to take care of the boundaries where the regions intersect. What is more interesting in our case is that we get an *explicit generating function*. Details are given in the Appendix.

A trivial consequence of Theorem 2.1 in [22] is that for every $r \in \mathbb{N}$, the sequence of moments $(\mathbb{E}\{(L_n(k)/n^k)^r\})_{n\in\mathbb{N}}$ converges to the constant $(r+1)^{-k}C_{r,k}$ as $n \to \infty$, whence, by the classical method of moments (see e.g. Example (d) on page 251 in [17]) the following convergence in distribution holds

$$\frac{L_n(k)}{n^k} \xrightarrow[n\to\infty]{d} Y_{\infty,k}, \tag{4}$$

where $Y_{\infty,k}$ is a random variable with values in $[0,1]$ such that $\mathbb{E}Y_{\infty,k}^r = (r+1)^{-k}C_{r,k}$ for all $r \in \mathbb{N}$. Conversely, since the sequence $(\frac{L_n(k)}{n^k})_{n\in\mathbb{N}}$ is uniformly bounded by 1, the convergence in distribution (4) yields the convergence of the moments, and thereby a particular case of Theorem 2.1 in [22] when restricted to power functions $f(n) = n^r$. The aforementioned Theorem 2.1 in [22] provides general conditions on a multiplicative function $f$ of a polynomial growth $r > -1$ that ensure the convergence of moments

$$\mathbb{E}\left\{\frac{f(L_n(k))}{n^{rk}}\right\}, \tag{5}$$

as $n \to \infty$, to a finite positive limit. The approach used in [22] to derive convergence of (5) is purely analytical. Even in the simple case (4) it does not shed light on the probabilistic mechanisms behind this convergence, nor on the probabilistic structure of the limit $Y_{\infty,k}$. Moreover, in general it does not provide a distributional convergence of

$$\frac{f(L_n(k))}{n^{rk}}, \quad k \in \mathbb{N}, \tag{6}$$

as $n \to \infty$. The main contributions of the current note is a derivation of a criterion for the convergence in distribution of (6), as $n \to \infty$, by using a purely probabilistic approach, see Theorem 2.3 below. Furthermore, we manage to identify the limit of (6) as an infinite product of independent random variables indexed by the set of prime numbers $\mathcal{P}$. Further comparison of our main results and Theorem 2.1 in [22] shall be given in Remark 2.5 below.

As we shall see, our main result is very close in spirit to a well-known result in probabilistic number theory, namely the celebrated Erdős–Wintner theorem, see for example [15] or Theorem 3 in [21]. Let us recall that the latter asserts that if $X^{(n)}$ is a random variable with uniform distribution on $\{1,2,\ldots,n\}$ and if $f$ is an *additive* arithmetic function, then the sequence $(f(X^{(n)}))_{n\in\mathbb{N}}$ converges in distribution if and only if the following three series converge for some $A > 0$:

$$\sum_{p\in\mathcal{P},\,|f(p)|>A} \frac{1}{p}, \qquad \sum_{p\in\mathcal{P},\,|f(p)|\leqslant A} \frac{f(p)}{p}, \qquad \sum_{p\in\mathcal{P},\,|f(p)|\leqslant A} \frac{f^2(p)}{p}. \tag{7}$$

Moreover, if the limit $X_\infty$ of $(f(X^{(n)}))_{n\in\mathbb{N}}$ exists, it necessarily satisfies

$$\mathbb{E}e^{itX_\infty} = \prod_{p\in\mathcal{P}} \left(1-\frac{1}{p}\right) \sum_{j=0}^{\infty} \frac{e^{itf(p^j)}}{p^j}, \quad t \in \mathbb{R},$$

and thus $X_\infty$ is a sum of independent random variables indexed by primes. The underlying probabilistic result behind the Erdős–Wintner result is Kolmogorov's three series theorem, see Chap. III.4 in [26]. Let us further point out that by

Kolmogorov's three series theorem, the conditions (7) are equivalent to the almost sure convergence of the series

$$\sum_{p\in\mathcal{P}} f\left(p^{\mathcal{G}(p)}\right), \tag{8}$$

where $(\mathcal{G}(p))_{p\in\mathcal{P}}$ is a family of mutually independent geometric random variables, such that

$$\mathbb{P}\{\mathcal{G}(p)=k\}=\left(1-\frac{1}{p}\right)\frac{1}{p^k},\quad k\in\mathbb{N}_0=\{0,1,2,\ldots\}. \tag{9}$$

Thus (8) is a representation of $f(X_\infty)$, the limit of $(f(X^{(n)}))_{n\in\mathbb{N}}$ as $n\to\infty$.

Let us finally mention two recent works [2, 10], where a closely related problem was addressed. In the cited papers the authors analyze an asymptotic behavior of $\operatorname{lcm}(A_n)$, where $A_n$ is a random subset of $\{1,2,\ldots,n\}$ obtained by removing every element with a fixed probability $p\in(0,1)$. Since in this case the cardinality of $A_n$ increases linearly as $n\to\infty$, the model exhibits a completely different asymptotic behavior, see e.g. Corollary 1.5 in [2].

We close the introduction by setting up some notation. We shall denote by $\lambda_p(n)$ the exponent of the prime number $p\in\mathcal{P}$ in the prime factorization of $n\in\mathbb{N}$, that is

$$n=\prod_{p\in\mathcal{P}} p^{\lambda_p(n)}.$$

Note that $\lambda_p(n)$ is zero for all but finitely many $p\in\mathcal{P}$. We shall further ubiquitously use the family $(\mathcal{G}_j(p))_{j\in\{1,\ldots,k\},p\in\mathcal{P}}$ of mutually independent random variables such that $\mathcal{G}_j(p)$ is distributed like $\mathcal{G}(p)$ in (9) for every $j=1,2,\ldots,k$. Finally, given any $i\in\mathbb{N}$, we shall denote by $\vee_{j=1}^{i}a_k$ the maximum of real numbers $a_1,\ldots,a_i$.

## 2. Main results

Given a multiplicative function $f$ and $r\in\mathbb{R}$, define the infinite random product

$$X_{f,\infty,k}:=\prod_{p\in\mathcal{P}}\frac{f(p^{\vee_{j=1}^{k}\mathcal{G}_j(p)})}{p^{r\sum_{j=1}^{k}\mathcal{G}_j(p)}}. \tag{10}$$

We characterize the convergence of $X_{f,\infty,k}$ in Proposition 2.1 below. The denominators in the infinite product (10) should be thought of as normalization factors. Note also that taking $f$ as the identity function and $r=1$, the quantity $X_{f,\infty,k}$ becomes

$$R_k:=\prod_{p\in\mathcal{P}} p^{\vee_{j=1}^{k}\mathcal{G}_j(p)-\sum_{j=1}^{k}\mathcal{G}_j(p)}\in 1/\mathbb{N}. \tag{11}$$

The ordinary generating function of $R_k^{-1}$ and the moments of $R_k$ will be computed in Proposition 2.6 and Proposition 2.7.

For $p\in\mathcal{P}$ and $r\in\mathbb{R}$, put

$$B_{p,r}=\log\left(\frac{|f(p)|}{p^r}\right). \tag{12}$$

**Proposition 2.1.** *The infinite product on the right-hand side of (10) converges a.s. if and only if the following three assumptions are satisfied: for some $A>0$,*

*(a) the series $\sum_{p\in\mathcal{P}}\frac{\mathbb{1}_{\{|B_{p,r}|\geqslant A\}}}{p}$ converges;*

(b) *the series* $\sum_{p\in\mathcal{P}} \frac{B_{p,r}\mathbb{1}_{\{|B_{p,r}|\leqslant A\}}}{p}$ *converges;*

(c) *the series* $\sum_{p\in\mathcal{P}} \frac{B_{p,r}^2\mathbb{1}_{\{|B_{p,r}|\leqslant A\}}}{p}$ *converges.*

*If moreover* $|f(p)| \sim p^r$ *as* $p \to \infty$ *along the prime numbers, then (a) holds automatically, (b) implies (c), and (b) is equivalent to*

(d) *the series* $\sum_{p\in\mathcal{P}} \frac{1}{p}\log\left(\frac{|f(p)|}{p^r}\right)$ *converges.*

*Remark* 2.2. Note that the assumption (i) in [22] implies $|f(p)| \sim p^r$ as $p \to \infty$ along the prime numbers, as well as (d).

In order to illustrate how demanding item (d) above is, let us recall the most classical result on the Bertrand-type series:

$$\sum_{p\in\mathcal{P}} \frac{1}{p\log^{1-\varepsilon} p} < \infty \quad \Longleftrightarrow \quad \varepsilon \leqslant 0.$$

The proof of Proposition 2.1, as well as proofs of all results from this section, are postponed to Section 3. With Proposition 2.1 at hand, we can formulate our main result.

**Theorem 2.3.** *Assume that* $f$ *is a multiplicative arithmetic function and that* $r \in \mathbb{R}$*. The following statements are equivalent:*

(i) *the infinite product* (10) *defining* $X_{f,\infty,k}$ *converges a.s.;*

(ii) *the conditions (a), (b) and (c) of Proposition 2.1 are satisfied;*

(iii) $X_{f,\infty,k}$ *converges a.s. and the following convergence in distribution holds*

$$\frac{f(L_n(k))}{\left(X_1^{(n)}X_2^{(n)}\cdots X_k^{(n)}\right)^r} \xrightarrow[n\to\infty]{d} X_{f,\infty,k}; \tag{13}$$

(iv) $X_{f,\infty,k}$ *converges a.s. and*

$$\frac{f(L_n(k))}{n^{rk}} \xrightarrow[n\to\infty]{d} X_{f,\infty,k}\prod_{j=1}^{k} U_j^r, \tag{14}$$

*where* $(U_j)_{j=1,\ldots,k}$ *are independent copies of a random variable* $U$ *with the uniform distribution on* $[0,1]$*, and* $(U_j)_{j=1,\ldots,k}$ *are also independent of* $X_{f,\infty,k}$*.*

*Remark* 2.4. The identity function $f(n) = n$ obviously satisfies assumptions (a), (b) and (c) with $r = 1$, thus with our notation (11),

$$\frac{L_n(k)}{X_1^{(n)}X_2^{(n)}\cdots X_k^{(n)}} \xrightarrow[n\to\infty]{d} R_k, \tag{15}$$

and

$$\frac{L_n(k)}{n^k} \xrightarrow[n\to\infty]{d} R_k\prod_{j=1}^{k} U_j = Y_{\infty,k}. \tag{16}$$

The quantity $R_k$ in (11) is a.s. positive. As we have already mentioned in the introduction, both (15) and (16) follow from the results of [22].

*Remark* 2.5. Let us now compare our Theorem 2.3 with Theorem 2.1 in [22] in more details. Whereas Hilberdink and Tóth's main focus is placed on the convergence of the first moments (5) of the variables (6) (and actually of *all* moments, because in (5) one may replace $f(L_n(k))/n^{rk}$ by $f(L_n(k))^q/n^{rkq}$), our Theorem 2.3 provides much less restrictive conditions, see Remark 2.2 above, ensuring the convergence in distribution of (6). Obviously, these results do overlap in some particular cases: convergence of moments can give convergence in distribution (e.g. if the method of moments applies, as for (4)); conversely, convergence in distribution may yield convergence of moments (for example, when the limit is compactly supported). But in general, they are of different nature. Furthermore, the limiting random variable (10), being almost surely finite under assumptions (a), (b) and (c) in Proposition 2.1, might have infinite power moments. Thereby in general we cannot expect convergence of the moments under (a), (b) and (c) alone. Another important observation is that we do not need any assumptions about the behavior of $f(p^q)$ for $q > 1$ (condition (ii) in [22]). Indeed, as we shall show in Section 3, powers of primes do not have impact in the a.s. convergence of the infinite product which defines $X_{f,\infty,k}$. Note that the same phenomenon occurs in the Erdős–Wintner theorem, see conditions (7). On the other hand, the behavior of $f(p^q)$ should impact the finiteness of power moments of $X_{f,\infty,k}$ explaining the appearance of condition (ii) in [22].

Let us close Section 2 by studying some properties of the random variable $R_k$ in (11). Plainly, it is an infinite product of blocks along primes $p \in \mathcal{P}$, each of them being equal to $1/p$ raised to the power $Z_k(p)$, where

$$Z_k(p) := \sum_{j=1}^{k} \mathcal{G}_j(p) - \vee_{j=1}^{k} \mathcal{G}_j(p). \tag{17}$$

Besides the very particular case $k = 2$, for which the latter reduces to $\mathcal{G}_1(p) \wedge \mathcal{G}_2(p)$ (and thus everything is known), the law of the random variable in (17) is not trivial. Let us mention in passing that quantities

$${}^{(r)}S_n = \xi_1 + \xi_2 + \cdots + \xi_n - \xi_n^{(1)} - \cdots - \xi_n^{(r)},$$

where $(\xi_k)_{k\in\mathbb{N}}$ are iid random variables and $\xi_n^{(n)} \leqslant \cdots \leqslant \xi_n^{(2)} \leqslant \xi_n^{(1)}$ is their arrangement in nondecreasing order, are called *trimmed sums*, see for instance [11]. However, we have not been able to locate in the vast body of literature on trimmed sums any results about the exact distribution of $Z_k(p)$.

**Proposition 2.6.** *Let $k \in \mathbb{N}$ and $p \in \mathcal{P}$. The ordinary generating function of $Z_k(p)$ is rational and is given for $|t| \leqslant p$ by*

$$\mathbb{E}t^{Z_k(p)} = \left(1 - \frac{1}{p}\right)^k \left(1 - \frac{t}{p}\right)^{-k} \sum_{j=1}^{k} \binom{k}{j} (-1)^{j-1} \frac{1 - \left(\frac{t}{p}\right)^j}{1 - \frac{t^{j-1}}{p^j}}.$$

*In particular, one has* $\mathbb{E}t^{Z_1(p)} = 1$, *as well as*

$$\mathbb{E}t^{Z_2(p)} = \mathbb{E}t^{\mathcal{G}_1(p)\wedge\mathcal{G}_2(p)} = \frac{1-\frac{1}{p^2}}{1-\frac{t}{p^2}},$$

$$\mathbb{E}t^{Z_3(p)} = \frac{\left(1-\frac{1}{p}\right)^2}{\left(1-\frac{t}{p^2}\right)\left(1-\frac{t^2}{p^3}\right)}\left(1+\frac{2}{p}+\frac{2t}{p^2}+\frac{t}{p^3}\right).$$

Notice that the expression of $\mathbb{E}t^{Z_2(p)}$ above is clear, as $\mathcal{G}_1(p)\wedge\mathcal{G}_2(p)$ is distributed as $\mathcal{G}(p^2)$.

Using Proposition 2.6 we immediately obtain the following corollary generalizing formulas (11) and (12) in [22].

**Corollary 2.7.** *For* $r \in \mathbb{N}_0$ *we have*

$$\mathbb{E}R_k^r = \mathbb{E}\prod_{p\in\mathcal{P}} p^{-rZ_k(p)} = \prod_{p\in\mathcal{P}} \frac{\left(1-\frac{1}{p}\right)^k}{\left(1-\frac{1}{p^{r+1}}\right)^k} \sum_{j=1}^{k} \binom{k}{j} (-1)^{j-1} \frac{1-\frac{1}{p^{j(r+1)}}}{1-\frac{1}{p^{(j-1)(r+1)+1}}}. \tag{18}$$

*In particular, using the Euler product of the Riemann zeta-function*

$$\zeta(s) = \prod_{p\in\mathcal{P}} \left(1-\frac{1}{p^s}\right)^{-1}, \quad \operatorname{Re} s > 1,$$

*we obtain* $\mathbb{E}R_1^r = 1$, *as well as*

$$C_{r,2} = \mathbb{E}R_2^r = \frac{\zeta(r+2)}{\zeta(2)},$$

$$C_{r,3} = \mathbb{E}R_3^r = \zeta(r+2)\zeta(2r+3)\prod_{p\in\mathcal{P}}\left(1-\frac{1}{p}\right)^2\left(1+\frac{2}{p}+\frac{2}{p^{r+2}}+\frac{1}{p^{r+3}}\right).$$

In general, it is not possible to further simplify the above Euler products. Notice that many well-known constants (in particular in number theory) have Euler product expansions, see e.g. [23, 24] and the whole Chap. 2 in [19].

## 3. Proofs

*Proof of Proposition 2.1.* Passing to logarithms, we see that the a.s. convergence of the infinite product is equivalent to the a.s. convergence of the series

$$\sum_{p\in\mathcal{P}} \left(\log\left|f(p^{\vee_{j=1}^k \mathcal{G}_j(p)})\right| - r\sum_{j=1}^{k}\mathcal{G}_j(p)\log p\right).$$

First of all, note that since $f(1) = 1$ it is enough to show that

$$\sum_{p\in\mathcal{P}} \left(\log\left|f(p^{\vee_{j=1}^k \mathcal{G}_j(p)})\right| - r\sum_{j=1}^{k}\mathcal{G}_j(p)\log p\right) \mathbb{1}_{\{\sum_{j=1}^k \mathcal{G}_j(p)\geqslant 1\}} \tag{19}$$

converges a.s. Further, we apply the Borel–Cantelli lemma to check that for any $k \geqslant 1$,

$$\mathbb{P}\left\{\sum_{j=1}^{k} \mathcal{G}_j(p) \geqslant 2 \text{ for infinitely many } p \in \mathcal{P}\right\} = 0. \tag{20}$$

Indeed,

$$\begin{aligned}
\sum_{p\in\mathcal{P}} \mathbb{P}\left\{\sum_{j=1}^{k} \mathcal{G}_j(p) \geqslant 2\right\} &= \sum_{p\in\mathcal{P}} \left(1 - \mathbb{P}\left\{\sum_{j=1}^{k} \mathcal{G}_j(p) = 0\right\} - \mathbb{P}\left\{\sum_{j=1}^{k} \mathcal{G}_j(p) = 1\right\}\right) \\
&= \sum_{p\in\mathcal{P}} \left(1 - \left(1-\frac{1}{p}\right)^k - k\left(1-\frac{1}{p}\right)^k \frac{1}{p}\right) \\
&= \sum_{p\in\mathcal{P}} \left(1 - \left(1-\frac{1}{p}\right)^k \left(1+\frac{k}{p}\right)\right) \\
&\leqslant \sum_{p\in\mathcal{P}} \left(1 - \left(1-\frac{k}{p}\right)\left(1+\frac{k}{p}\right)\right) = k^2 \sum_{p\in\mathcal{P}} \frac{1}{p^2} < \infty.
\end{aligned}$$

Thus, the event $\{\sum_{j=1}^{k} \mathcal{G}_j(p) \geqslant 2\}$ occurs only for finitely many $p \in \mathcal{P}$ a.s. and the convergence of (19) is equivalent to that of

$$\sum_{p\in\mathcal{P}} (\log|f(p)| - r\log p)\, \mathbb{1}_{\{\sum_{j=1}^{k} \mathcal{G}_j(p)=1\}} = \sum_{p\in\mathcal{P}} B_{p,r}\, \mathbb{1}_{\{\sum_{j=1}^{k} \mathcal{G}_j(p)=1\}}, \tag{21}$$

because obviously the event $\{\sum_{j=1}^{k} \mathcal{G}_j(p) = 1\}$ implies $\{\vee_{j=1}^{k} \mathcal{G}_j(p) = 1\}$. Note that the series in (21) consists of independent summands. Therefore, the assumptions (i), (ii) and (iii) are necessary and sufficient for the a.s. convergence of (21) by Kolmogorov's three series theorem (see page 317 in [17]), since

$$\mathbb{P}\left\{\sum_{j=1}^{k} \mathcal{G}_j(p) = 1\right\} = k\left(1-\frac{1}{p}\right)^k \frac{1}{p} \sim \frac{k}{p}, \quad p \to \infty. \qquad \square$$

The main ingredient in the subsequent proofs is contained in the following elementary lemma. Its first part is well known in the probabilistic literature and is given explicitly in [4], see formula (1.45) on page 28 therein. The second and third parts are just slight extensions thereof. Recall that $X^{(n)}$ denotes a random variable with uniform distribution on $\{1, 2, \ldots, n\}$.

**Lemma 3.1.** *Let*

$$X^{(n)} = \prod_{p\in\mathcal{P}} p^{\lambda_p(X^{(n)})}$$

*be the decomposition of* $X^{(n)} \in \{1, 2, \ldots, n\}$ *into prime factors. Then*

*(i) we have*

$$\left(\lambda_p(X^{(n)})\right)_{p\in\mathcal{P}} \xrightarrow[n\to\infty]{d} \left(\mathcal{G}(p)\right)_{p\in\mathcal{P}};$$

*(ii) we have*

$$\left(\frac{X^{(n)}}{n}, \left(\lambda_p(X^{(n)})\right)_{p\in\mathcal{P}}\right) \xrightarrow[n\to\infty]{d} \left(U, \left(\mathcal{G}(p)\right)_{p\in\mathcal{P}}\right),$$

*with $U$ being uniformly distributed on $[0,1]$ and independent of $(\mathcal{G}(p))_{p\in\mathcal{P}}$;*
*(iii) for $p,q\in\mathcal{P}$, $p\neq q$ and $k_p,k_q\in\mathbb{N}_0$, we have*

$$\mathbb{P}\{\lambda_p(X^{(n)})=k_p,\lambda_q(X^{(n)})=k_q\}=\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\frac{1}{p^{k_p}q^{k_q}}+O\left(\frac{1}{n}\right),$$

*where the constant in the $O$-term does not depend on $(p,q,k_p,k_q)$.*

*Proof.* Let us prove part (ii). Fix $x\in(0,1]$, $p\in\mathcal{P}$ and $c_2,c_3,\ldots,c_p\in\mathbb{N}_0$. One has

$$\begin{aligned}
&\mathbb{P}\{X^{(n)}\leqslant nx,\lambda_2(X^{(n)})\geqslant c_2,\lambda_3(X^{(n)})\geqslant c_3,\ldots,\lambda_p(X^{(n)})\geqslant c_p\}\\
&\qquad=\mathbb{P}\{X^{(n)}\leqslant\lfloor nx\rfloor,X^{(n)}\text{ is divisible by }2^{c_2}3^{c_3}\cdots p^{c_p}\}\\
&\qquad=\frac{1}{n}\#\{k\in\{1,2,\ldots,\lfloor nx\rfloor\}:k\text{ is divisible by }2^{c_2}3^{c_3}\cdots p^{c_p}\}\\
&\qquad=\frac{1}{n}\left\lfloor\frac{\lfloor nx\rfloor}{2^{c_2}3^{c_3}\cdots p^{c_p}}\right\rfloor\\
&\qquad\underset{n\to\infty}{\longrightarrow}\frac{x}{2^{c_2}3^{c_3}\cdots p^{c_p}}=\mathbb{P}\{U\leqslant x,\mathcal{G}(2)\geqslant c_2,\mathcal{G}(3)\geqslant c_3,\ldots,\mathcal{G}(p)\geqslant c_p\}.
\end{aligned}$$

Part (i) obviously follows from part (ii). For the item (iii), notice that

$$\mathbb{P}\{\lambda_p(X^{(n)})\geqslant i,\lambda_q(X^{(n)})\geqslant j\}=\frac{1}{n}\left\lfloor\frac{n}{p^iq^j}\right\rfloor\in\left(\frac{1}{p^iq^j}-\frac{1}{n},\frac{1}{p^iq^j}\right]$$

and thus

$$\begin{aligned}
&\mathbb{P}\{\lambda_p(X^{(n)})=k_p,\lambda_q(X^{(n)})=k_q\}\\
&\qquad\in\left[\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\frac{1}{p^{k_p}q^{k_q}}-\frac{2}{n},\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\frac{1}{p^{k_p}q^{k_q}}+\frac{2}{n}\right].
\end{aligned}$$

The proof is complete. □

*Proof of Theorem 2.3.* With Lemma 3.1 at hand, the proof of Theorem 2.3 is more or less straightforward. From Proposition 2.1, we already know that (i) and (ii) are equivalent.

Let us show that (i) implies (iii). Let us first write the prime power decompositions

$$X_j^{(n)}=\prod_{p\in\mathcal{P}}p^{\lambda_p(X_j^{(n)})},\quad j=1,\ldots,k.$$

Then

$$L_n(k)=\operatorname{lcm}\{X_1^{(n)},\ldots,X_k^{(n)}\}=\prod_{p\in\mathcal{P}}p^{\vee_{j=1}^k\lambda_p(X_j^{(n)})},$$

and, using multiplicativity of $f$,

$$\frac{f(L_n(k))}{\left(X_1^{(n)}X_2^{(n)}\cdots X_k^{(n)}\right)^r}=\prod_{p\in\mathcal{P}}\frac{f(p^{\vee_{j=1}^k\lambda_p(X_j^{(n)})})}{p^{r\sum_{j=1}^k\lambda_p(X_j^{(n)})}}.$$

Fix $m\in\mathbb{N}$ and decompose

$$\frac{f(L_n(k))}{\left(X_1^{(n)}X_2^{(n)}\cdots X_k^{(n)}\right)^r}=\left(\prod_{p\in\mathcal{P},\,p\leqslant m}\cdots\right)\left(\prod_{p\in\mathcal{P},\,p>m}\cdots\right)=:Y_m(n)Z_m(n).$$

By Lemma 3.1 (i) and the continuous mapping theorem, see Theorem 2.7 in [5],

$$Y_m(n) \xrightarrow[n\to\infty]{d} X_{f,\infty,k}(m) := \prod_{p\in\mathcal{P},\, p\leqslant m} \frac{f(p^{\vee_{j=1}^k \mathcal{G}_j(p)})}{p^{r\sum_{j=1}^k \mathcal{G}_j(p)}}.$$

By (i) we have

$$X_{f,\infty,k}(m) \xrightarrow[m\to\infty]{a.s.} X_{f,\infty,k}.$$

Denoting by $E_\varepsilon$ the event $\{|\log(|Z_m(n)|)| > \varepsilon\}$ and using Thmeorem 3.2 in [5], it remains to show that for every fixed $\varepsilon > 0$,

$$\lim_{m\to\infty} \limsup_{n\to\infty} \mathbb{P}\{E_\varepsilon\} = 0. \tag{22}$$

We have

$$\begin{aligned}
\mathbb{P}\{E_\varepsilon\} &= \mathbb{P}\left\{\text{for some } p\in\mathcal{P},\, p>m, \sum_{j=1}^k \lambda_p(X_j^{(n)}) \geqslant 2, E_\varepsilon\right\} \\
&\quad + \mathbb{P}\left\{\text{for all } p\in\mathcal{P},\, p>m, \sum_{j=1}^k \lambda_p(X_j^{(n)}) \leqslant 1, E_\varepsilon\right\} \\
&\leqslant \sum_{p\in\mathcal{P},\, p>m} \mathbb{P}\left\{\sum_{j=1}^k \lambda_p(X_j^{(n)}) \geqslant 2\right\} \\
&\quad + \mathbb{P}\left\{\left|\sum_{p\in\mathcal{P},\, p>m} B_{p,r}\mathbb{1}_{\{\sum_{j=1}^k \lambda_p(X_j^{(n)})=1\}}\right| > \varepsilon\right\} =: P_m^{(1)}(n) + P_m^{(2)}(n).
\end{aligned}$$

We deal with the latter two summands separately. For $P_m^{(1)}(n)$, we have

$$\begin{aligned}
P_m^{(1)}(n) &\leqslant \sum_{p\in\mathcal{P},\, p>m} \mathbb{P}\{\lambda_p(X_j^{(n)}) \geqslant 2 \text{ for some } j=1,\dots,k\} \\
&\quad + \sum_{p\in\mathcal{P},\, p>m} \mathbb{P}\{\lambda_p(X_i^{(n)}) \geqslant 1, \lambda_p(X_j^{(n)}) \geqslant 1 \text{ for some } 1\leqslant i,j\leqslant k, i\neq j\} \\
&\leqslant k \sum_{p\in\mathcal{P},\, p>m} \mathbb{P}\{\lambda_p(X^{(n)}) \geqslant 2\} + k(k-1) \sum_{p\in\mathcal{P},\, p>m} (\mathbb{P}\{\lambda_p(X^{(n)}) \geqslant 1\})^2 \\
&= k \sum_{p\in\mathcal{P},\, p>m} \frac{1}{n}\left\lfloor \frac{n}{p^2}\right\rfloor + k(k-1) \sum_{p\in\mathcal{P},\, p>m} \left(\frac{1}{n}\left\lfloor\frac{n}{p}\right\rfloor\right)^2 \\
&\leqslant k^2 \sum_{p\in\mathcal{P},\, p>m} \frac{1}{p^2} \to 0, \quad m\to\infty.
\end{aligned}$$

To deal with $P_m^{(2)}(n)$ we pick $A>0$ such that the conditions (a), (b) and (c) in Proposition 2.1 hold. We have

$$\begin{aligned} P_m^{(2)}(n) &\leqslant \mathbb{P}\left\{\left|\sum_{p\in\mathcal{P},\,p>m} B_{p,r}\mathbb{1}_{\{|B_{p,r}|\geqslant A,\sum_{j=1}^k \lambda_p(X_j^{(n)})=1\}}\right|>\frac{\varepsilon}{2}\right\} \\ &\quad+\mathbb{P}\left\{\left|\sum_{p\in\mathcal{P},\,p>m} B_{p,r}\mathbb{1}_{\{|B_{p,r}|\leqslant A,\sum_{j=1}^k \lambda_p(X_j^{(n)})=1\}}\right|>\frac{\varepsilon}{2}\right\} \\ &\leqslant \mathbb{P}\left\{\text{for some } p\in\mathcal{P},\,p>m,|B_{p,r}|\geqslant A,\sum_{j=1}^k\lambda_p(X_j^{(n)})=1\right\} \\ &\quad+\mathbb{P}\left\{\left|\sum_{p\in\mathcal{P},\,p>m} B_{p,r}\mathbb{1}_{\{|B_{p,r}|\leqslant A,\sum_{j=1}^k \lambda_p(X_j^{(n)})=1\}}\right|>\frac{\varepsilon}{2}\right\}. \end{aligned} \tag{23}$$

The first probability can be estimated as follows

$$\begin{aligned} &\mathbb{P}\left\{\text{for some } p\in\mathcal{P},\,p>m,|B_{p,r}|\geqslant A,\sum_{j=1}^k\lambda_p(X_j^{(n)})=1\right\} \\ &\qquad\leqslant \sum_{p\in\mathcal{P},\,p>m}\mathbb{1}_{\{|B_{p,r}|\geqslant A\}}\mathbb{P}\left\{\sum_{j=1}^k\lambda_p(X_j^{(n)})=1\right\} \\ &\qquad\leqslant \sum_{p\in\mathcal{P},\,p>m}\mathbb{1}_{\{|B_{p,r}|\geqslant A\}}k\mathbb{P}\left\{\lambda_p(X^{(n)})\geqslant 1\right\} \\ &\qquad= k\sum_{p\in\mathcal{P},\,p>m}\mathbb{1}_{\{|B_{p,r}|\geqslant A\}}\frac{1}{n}\left\lfloor\frac{n}{p}\right\rfloor \\ &\qquad\leqslant k\sum_{p\in\mathcal{P},\,p>m}\frac{\mathbb{1}_{\{|B_{p,r}|\geqslant A\}}}{p}\to 0, \end{aligned}$$

as $m\to\infty$, by assumption (a) in Proposition 2.1.

It remains to check that

$$\lim_{m\to\infty}\limsup_{n\to\infty}\mathbb{P}\left\{\left|\sum_{p\in\mathcal{P},\,p>m} B_{p,r}\mathbb{1}_{\{|B_{p,r}|\leqslant A,\sum_{j=1}^k \lambda_p(X_j^{(n)})=1\}}\right|>\frac{\varepsilon}{2}\right\}=0, \tag{24}$$

see (23). To that aim, we first notice that

$$\left\{\sum_{j=1}^k\lambda_p(X_j^{(n)})=1\right\}=\bigcup_{j=1}^k\left\{\lambda_p(X_j^{(n)})=1,\lambda_p(X_i^{(n)})=0,\forall i\neq j\right\}=:\bigcup_{j=1}^k C_{j,p,n}.$$

Moreover, the events $(C_{j,p,n})_{j=1,\ldots,k}$ are disjoint and equiprobable. Thus, the limit (24) follows if we can check that

$$\lim_{m\to\infty}\limsup_{n\to\infty}\mathbb{P}\left\{\left|\sum_{p\in\mathcal{P},\,p>m} B'_{p,r}\mathbb{1}_{C_{1,p,n}}\right|>\frac{\varepsilon}{2k}\right\}=0,$$

where $B'_{p,r}:=B_{p,r}\mathbb{1}_{\{|B_{p,r}|\leqslant A\}}$.

Keeping in mind that $\lambda_p(X^{(n)}) = 0$ for $p > n$, we see that that it is enough to prove that

$$\lim_{m\to\infty} \limsup_{n\to\infty} \mathbb{P}\left\{ \left| \sum_{p\in\mathcal{P},\, p\in(m,\sqrt{n}]} B'_{p,r} \mathbb{1}_{C_{1,p,n}} \right| > \frac{\varepsilon}{4k} \right\} = 0 \tag{25}$$

as well as

$$\lim_{m\to\infty} \limsup_{n\to\infty} \mathbb{P}\left\{ \left| \sum_{p\in\mathcal{P},\, p\in(\sqrt{n},n]} B'_{p,r} \mathbb{1}_{C_{1,p,n}} \right| > \frac{\varepsilon}{4k} \right\} = 0. \tag{26}$$

Note that $C_{1,p,n} \cap C_{1,q,n} = \varnothing$ if $p, q > \sqrt{n}$, thus (26) is equivalent to

$$\lim_{m\to\infty} \limsup_{n\to\infty} \mathbb{P}\left\{ \sum_{p\in\mathcal{P},\, p\in(\sqrt{n},n]} (B'_{p,r})^2 \mathbb{1}_{C_{1,p,n}} > \frac{\varepsilon^2}{16k^2} \right\} = 0.$$

The latter relation follows from Markov's inequality, since

$$\begin{aligned}
&\mathbb{P}\left\{ \sum_{p\in\mathcal{P},\, p\in(\sqrt{n},n]} (B'_{p,r})^2 \mathbb{1}_{C_{1,p,n}} > \frac{\varepsilon^2}{16k^2} \right\} \\
&\qquad \leqslant \frac{16k^2}{\varepsilon^2} \sum_{p\in\mathcal{P},\, p\in(\sqrt{n},n]} (B'_{p,r})^2 \mathbb{P}\{C_{1,p,n}\} \\
&\qquad \leqslant \frac{16k^2}{\varepsilon^2} \sum_{p\in\mathcal{P},\, p\in(n,\sqrt{n}]} (B'_{p,r})^2 \mathbb{P}\{\lambda_p(X_1^{(n)}) \geqslant 1\} \\
&\qquad = \frac{16k^2}{\varepsilon^2} \sum_{p\in\mathcal{P},\, p\in(n,\sqrt{n}]} B_{p,r}^2 \mathbb{1}_{\{|B_{p,r}|\leqslant A\}} \frac{1}{n} \left\lfloor \frac{n}{p} \right\rfloor \\
&\qquad \leqslant \frac{16k^2}{\varepsilon^2} \sum_{p\in\mathcal{P},\, p\in(n,\sqrt{n}]} \frac{B_{p,r}^2 \mathbb{1}_{\{|B_{p,r}|\leqslant A\}}}{p}.
\end{aligned}$$

The latter sum converges to zero as $n \to \infty$, by assumption (c) in Proposition 2.1.

In order to derive (25), we again use Markov's inequality to obtain

$$\mathbb{P}\left\{ \left| \sum_{p\in\mathcal{P},\, p\in(m,\sqrt{n}]} B'_{p,r} \mathbb{1}_{C_{1,p,n}} \right| > \frac{\varepsilon}{4k} \right\} \leqslant \frac{16k^2}{\varepsilon^2} \mathbb{E}\left\{ \left( \sum_{p\in\mathcal{P},\, p\in(m,\sqrt{n}]} B'_{p,r} \mathbb{1}_{C_{1,p,n}} \right)^2 \right\},$$

and, further,

$$\begin{aligned}
&\mathbb{E}\left\{ \left( \sum_{p\in\mathcal{P},\, p\in(m,\sqrt{n}]} B'_{p,r} \mathbb{1}_{C_{1,p,n}} \right)^2 \right\} \\
&= \sum_{p\in\mathcal{P},\, p\in(m,\sqrt{n}]} (B'_{p,r})^2 \mathbb{P}\{C_{1,p,n}\} + \sum_{p,q\in\mathcal{P},\, p,q\in(m,\sqrt{n}],\, p\neq q} B'_{p,r} B'_{q,r} \mathbb{P}\{C_{1,p,n} \cap C_{1,q,n}\}.
\end{aligned}$$

We have already estimated the first sum, and thus focus only on the second one. Firstly, as $pq \leqslant n$ and using part (iii) of Lemma 3.1, we may write

$$\begin{aligned}
&\mathbb{P}\{C_{1,p,n} \cap C_{1,q,n}\} \\
&= \mathbb{P}\{\lambda_p(X_1^{(n)}) = 1, \lambda_q(X_1^{(n)}) = 1\}(\mathbb{P}\{\lambda_p(X_1^{(n)}) = 0, \lambda_q(X_1^{(n)}) = 0\})^{k-1} \\
&= \left(\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\frac{1}{pq} + O\left(\frac{1}{n}\right)\right)\left(\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right) + O\left(\frac{1}{n}\right)\right)^{k-1} \\
&= \left(1-\frac{1}{p}\right)^k \left(1-\frac{1}{q}\right)^k \frac{1}{pq} + O\left(\frac{1}{n}\right).
\end{aligned}$$

With the above expansion at hand, we have

$$\begin{aligned}
&\sum_{p,q\in\mathcal{P},\, p,q\in(m,\sqrt{n}],\, p\neq q} B'_{p,r}B'_{q,r}\mathbb{P}\{C_{1,p,n} \cap C_{1,q,n}\} \\
&\qquad = \sum_{p,q\in\mathcal{P},\, p,q\in(m,\sqrt{n}],\, p\neq q} \left(\left(1-\frac{1}{p}\right)^k \frac{B'_{p,r}}{p}\right)\left(\left(1-\frac{1}{q}\right)^k \frac{B'_{q,r}}{q}\right) \\
&\qquad\quad + O\left(\frac{1}{n} \sum_{p,q\in\mathcal{P},\, p,q\in(m,\sqrt{n}],\, p\neq q} 1\right).
\end{aligned}$$

With $\pi(x)$ denoting the number of primes $p \leqslant x$, we have

$$\frac{1}{n} \sum_{p,q\in\mathcal{P},\, p,q\in(m,\sqrt{n}]} 1 \leqslant \frac{1}{n} \sum_{p,q\in\mathcal{P},\, p,q\leqslant\sqrt{n}} 1 \leqslant \frac{1}{n}\pi(\sqrt{n})^2 \to 0$$

as $n \to \infty$, since $\pi(x) = o(x)$ as $x \to \infty$ by the prime number theorem.

Finally, using assumption (b) of Proposition 2.1, we see that

$$\begin{aligned}
&\lim_{m\to\infty} \limsup_{n\to\infty} \sum_{p,q\in\mathcal{P},\, p,q\in(m,\sqrt{n}]} \left(\left(1-\frac{1}{p}\right)^k \frac{B'_{p,r}}{p}\right)\left(\left(1-\frac{1}{q}\right)^k \frac{B'_{q,r}}{q}\right) \\
&\qquad = \lim_{m\to\infty} \limsup_{n\to\infty} \left(\sum_{p\in\mathcal{P},\, p\in(m,\sqrt{n}]} \left(\left(1-\frac{1}{p}\right)^k \frac{B'_{p,r}}{p}\right)\right)^2 \\
&\qquad = 0,
\end{aligned}$$

and (25) follows.

Summarizing, we see that (i) implies (iii). To see that (iii) implies (iv), just note that by Lemma 3.1 (ii) and (iii), we have

$$\left(\frac{f(L_n(k))}{\left(X_1^{(n)}X_2^{(n)}\cdots X_k^{(n)}\right)^r}, \frac{X_1^{(n)}}{n}, \ldots, \frac{X_k^{(n)}}{n}\right) \xrightarrow[n\to\infty]{d} (X_{f,\infty,k}, U_1, \ldots, U_k).$$

Therefore, (14) follows by the continuity of multiplication and the continuous mapping theorem. Obviously, (iv) implies (i). The proof of Theorem 2.3 is complete. □

*Proof of Proposition 2.6.* We start with an auxiliary lemma, which in our opinion is interesting in its own and will be extended in Appendix A to more general Diophantine equations.

**Lemma 3.2.** *Let $k \in \mathbb{N}$ and $\ell, m \in \mathbb{N}_0$ be fixed integers. Then*

$$\sum_{a_1,\dots,a_k=0}^{\infty} \mathbb{1}_{\{a_1+\cdots+a_k=\ell, \vee_{j=1}^k a_j \leqslant m\}} = [z^\ell] \left(\frac{1-z^{m+1}}{1-z}\right)^k \tag{27}$$

*and*

$$\sum_{a_1,\dots,a_k=0}^{\infty} \mathbb{1}_{\{a_1+\cdots+a_k=\ell, \vee_{j=1}^k a_j = m\}} = [z^\ell] \left(\left(\frac{1-z^{m+1}}{1-z}\right)^k - \left(\frac{1-z^{m}}{1-z}\right)^k\right). \tag{28}$$

*Proof.* It is known that the number of compositions of $\ell$ into $i \in \mathbb{N}_0$ summands from the set $\{1, 2, \dots, m\}$ is given by

$$[z^\ell] \left(z\left(\frac{1-z^m}{1-z}\right)\right)^i,$$

see e.g. **I.15** on page 45 in [20]. Note that the quantity on the left-hand side of (27) is equal to the number of compositions of $\ell$ into $k$ summands from the set $\{0, 1, 2, \dots, m\}$. Let $i \in \{0, \dots, k\}$ be the number of non-zero summands. Then

$$\begin{aligned}
\sum_{a_1,\dots,a_k=0}^{\infty} \mathbb{1}_{\{a_1+\cdots+a_k=l, \vee_{j=1}^k a_j \leqslant m\}} &= \sum_{i=0}^{k} \binom{k}{i} [z^\ell] \left(z\left(\frac{1-z^m}{1-z}\right)\right)^i \\
&= [z^\ell] \sum_{i=0}^{k} \binom{k}{i} \left(z\left(\frac{1-z^m}{1-z}\right)\right)^i \\
&= [z^\ell] \left(1 + z\left(\frac{1-z^m}{1-z}\right)\right)^k \\
&= [z^\ell] \left(\frac{1-z^{m+1}}{1-z}\right)^k,
\end{aligned}$$

which proves (27). Formula (28) follows by subtraction. □

Now we are in position to prove Proposition 2.6. We have:

$$\begin{aligned}
\mathbb{E}t^{Z_k(p)} &= \sum_{\ell=0}^{\infty} t^\ell \sum_{a_1,\dots,a_k=0}^{\infty} \left(1-\frac{1}{p}\right)^k \frac{1}{p^{a_1+\cdots+a_k}} \mathbb{1}_{\{a_1+\cdots+a_k-\vee_{j=1}^k a_j = \ell\}} \\
&= \left(1-\frac{1}{p}\right)^k \sum_{\ell=0}^{\infty} t^\ell \sum_{m=0}^{\infty} \sum_{a_1,\dots,a_k=0}^{\infty} \frac{1}{p^{\ell+m}} \mathbb{1}_{\{a_1+\cdots+a_k=\ell+m, \vee_{j=1}^k a_j = m\}} \\
&= \left(1-\frac{1}{p}\right)^k \sum_{\ell=0}^{\infty} \left(\frac{t}{p}\right)^\ell \sum_{m=0}^{\infty} p^{-m} \sum_{a_1,\dots,a_k=0}^{\infty} \mathbb{1}_{\{a_1+\cdots+a_k=\ell+m, \vee_{j=1}^k a_j = m\}}.
\end{aligned}$$

Using Lemma 3.2 we continue as follows

$$\begin{aligned}\mathbb{E}t^{Z_k(p)} &= \left(1-\frac{1}{p}\right)^k \sum_{m=0}^{\infty} p^{-m} \sum_{l=0}^{\infty} (t/p)^l [z^{l+m}] \left[ \left( \frac{1-z^{m+1}}{1-z} \right)^k - \left( \frac{1-z^m}{1-z} \right)^k \right] \\ &= \left(1-\frac{1}{p}\right)^k \sum_{m=0}^{\infty} p^{-m} \sum_{l=0}^{\infty} (t/p)^l [z^{l}] \left[ z^{-m} \left( \left( \frac{1-z^{m+1}}{1-z} \right)^k - \left( \frac{1-z^m}{1-z} \right)^k \right) \right] \\ &= \left(1-\frac{1}{p}\right)^k \sum_{m=0}^{\infty} t^{-m} \left[ \left( \left( \frac{1-(t/p)^{-(m+1)}}{1-t/p} \right)^k - \left( \frac{1-(t/p)^{-m}}{1-t/p} \right)^k \right) \right],\end{aligned}$$

where the last equality follows by evaluating the term in square brackets at $z = t/p$. The claim of lemma is now a simple consequence of the binomial theorem and subsequent evaluation of resulting geometric series. □

## Appendix A. On a Diophantine equation

In passing, the proof of Proposition 2.6 shows that the number $q_l$ of solutions $(a_1, \ldots, a_k) \in \mathbb{N}_0^k$ of the Diophantine equation

$$a_1 + \cdots + a_k - \vee_{j=1}^k a_j = \ell, \quad \ell \in \mathbb{N}, \tag{29}$$

has a rational generating function which can be expressed as follows:

$$\sum_{\ell=0}^{\infty} q_\ell t^\ell = \sum_{m=0}^{\infty} t^{-m} \left( \left( \frac{1-t^{m+1}}{1-t} \right)^k - \left( \frac{1-t^m}{1-t} \right)^k \right).$$

This may be generalized in the following way. For fixed $(x_1, \ldots, x_k) \in \mathbb{N}^k$ and $b \in \mathbb{N}$, consider the Diophantine equation

$$x_1 a_1 + \cdots + x_k a_k - b \vee_{j=1}^k a_j = \ell \tag{30}$$

and denote by $q_\ell$ the number of solutions $(a_1, \ldots, a_k) \in \mathbb{N}_0^k$ to (30).

**Theorem A.1.** *We have*

$$f_{k,b}^{(x_i)}(t) := \sum_{\ell=0}^{\infty} q_\ell t^\ell = \sum_{m=0}^{\infty} t^{-bm} \left( \prod_{j=1}^k \frac{1-t^{(m+1)x_j}}{1-t^{x_j}} - \prod_{i=1}^k \frac{1-t^{mx_j}}{1-t^{x_j}} \right), \quad |t| < 1.$$

*In particular, the generating function $f_{k,b}^{(x_i)}$ is rational.*

*Proof.* Decomposing upon the value of the maximum of $a_1, \ldots, a_k$, one may write

$$\begin{aligned} f_{k,b}^{(x_i)}(t) &= \sum_{a_1,\ldots,a_k=0}^{\infty} t^{x_1 a_1 + \cdots + x_k a_k - b \vee_{j=1}^k a_j} \\ &= \sum_{m=0}^{\infty} t^{-bm} \sum_{a_1,\ldots,a_k=0}^{\infty} t^{x_1 a_1 + \cdots + x_k a_k} \mathbb{1}_{\{\vee_{j=1}^k a_j = m\}}. \end{aligned}$$

Further,

$$\sum_{a_1,\ldots,a_k=0}^{\infty} t^{x_1 a_1 + \cdots + x_k a_k} \mathbb{1}_{\{\vee_{j=1}^k a_j = m\}} = T_{k,m}^{(x_i)}(t) - T_{k,m-1}^{(x_i)}(t),$$

where we have put

$$T_{k,m}^{(x_i)}(t) = \sum_{a_1,\dots,a_k=0}^{\infty} t^{x_1a_1+\cdots+x_ka_k} \mathbb{1}_{\{\vee_{j=1}^k a_j \leqslant m\}}.$$

It remains to apply formula (6) in [16], which is an extension of (27), to obtain

$$T_{k,m}^{(x_i)}(t) = \prod_{j=1}^{k} \sum_{s=0}^{m} t^{sa_j} = \prod_{j=1}^{k} \frac{1-t^{(m+1)a_j}}{1-t^{a_j}}. \qquad \square$$

## Acknowledgments

We would like to thank Djalil Chafaï and Richard Stanley for interesting discussions.

## References

[1] Abramovich, S. and Nikitin, Y. Yu. (2017). On the probability of coprimality of two natural numbers chosen at random: from Euler identity to Haar measure on the ring of adeles. *Bernoulli News*, **24**, 7–13.

[2] Alsmeyer, G., Kabluchko, Z. and Marynych, A. (2018). Limit theorems for the least common multiple of a random set of integers. Preprint available at https://arxiv.org/abs/1801.08934.

[3] Apostol, T. (1976). *Introduction to analytic number theory.* Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg.

[4] Arratia, R., Barbour, A. D. and Tavaré, S. (2003). *Logarithmic Combinatorial Structures: a Probabilistic Approach.* EMS Monographs in Mathematics. European Mathematical Society.

[5] Billingsley, P. (1999). *Convergence of probability measures.* Second edition. Wiley Series in Probability and Statistics: Probability and Statistics. John Wiley & Sons.

[6] Bingham, N. H., Goldie, C. M. and Teugels, J. L. (1989). *Regular variation.* Encyclopedia of Mathematics and its Applications, 27. Cambridge University Press.

[7] Cesàro, E. (1884). Probabilités de certains faits arithmétiques. *Mathesis*, **4**, 150–151.

[8] Cesàro, E. (1885). Sur le plus grand commun diviseur de plusieurs nombres. *Ann. Mat. Pura Appl.*, **13**, 291–294.

[9] Cesàro, E. (1885). Étude moyenne du plus grand commun diviseur de deux nombres. *Ann. Mat. Pura Appl.*, **13**, 235–250.

[10] Cilleruelo, J., Rué, J., Šarka, P. and Zumalacárregui, A. (2014). The least common multiple of random sets of positive integers. *J. Numb. Theory*, **144**, 92–104.

[11] Csörgő, S. and Simons, G. (1995). Precision calculation of distributions for trimmed sums. *Ann. Appl. Probab.*, **5**, no. 3, 854–873.

[12] Diaconis, P. and Erdős, P. (2004). On the distribution of the greatest common divisor. *Lecture Notes Monogr. Ser.*, **45**, 56–61.

[13] Dirichlet, G. L. (1849). Über die Bestimmung der mittleren Werthe in der Zahlentheorie. *Abhandlungen der Königlich Preussischen Akademie der Wissenschaften*, 69–83.

[14] Ehrhart, E. (1967). Sur un problème de géométrie diophantienne linéaire. I. Polyèdres et réseaux. *J. Reine Angew. Math.*, **226**, 1–29.
[15] Erdős, P. and Wintner, A. (1939). Additive arithmetical functions and statistical independence. *Amer. J. Math.*, **61**, 713–721.
[16] Faaland, B. (1972). On the number of solutions to a Diophantine equation. *J. Combinatorial Theory Ser. A*, **13**, 170–175.
[17] Feller, W. (1971). *An introduction to probability theory and its applications. Vol. II.* Second edition John Wiley & Sons, Inc., New York-London-Sydney.
[18] Fernández, J. and Fernández, P. (2013). On the probability distribution of the gcd and lcm of $r$-tuples of integers. Preprint available at https://arxiv.org/abs/1305.0536.
[19] Finch, S. R. (2009). *Mathematical constants.* Encyclopedia of Mathematics and its Applications, 94. Cambridge University Press.
[20] Flajolet, P. and Sedgewick, R. (2009). *Analytic Combinatorics.* Cambridge University Press.
[21] Galambos, J. (1970). Distribution of arithmetical functions. A survey. *Ann. Inst. H. Poincaré Sect. B*, **6**, 281–305.
[22] Hilberdink, T. and Tóth, L. (2016). On the average value of the least common multiple of $k$ positive integers. *J. Numb. Theory*, **169**, 327–341.
[23] Moree, P. (2000). Approximation of singular series and automata. With an appendix by Niklasch, G. *Manuscripta Math.*, **101**, no. 3, 385–399.
[24] Niklasch, G. (2002). Some number-theoretical constants arising as products of rational functions of $p$ over primes. Preprint available at https://oeis.org/A001692/a001692.html
[25] Nymann, J. E. (1972). On the probability that $k$ positive integers are relatively prime. *J. Numb. Theory*, **4**, 469–473.
[26] Tenenbaum, G. (1995). *Introduction to analytic and probabilistic number theory.* Cambridge Studies in Advanced Mathematics, 46. Cambridge University Press.

Alin Bostan, Inria, Université Paris-Saclay, 1 rue Honoré d'Estienne d'Orves, 91120 Palaiseau, France
*E-mail address*: alin.bostan@inria.fr

Alexander Marynych, Faculty of Computer Science and Cybernetics, Taras Shevchenko National University of Kyiv, 01601 Kyiv, Ukraine
*E-mail address*: marynych@unicyb.kiev.ua

Kilian Raschel, CNRS & Institut Denis Poisson, Université de Tours and Université d'Orléans, 37200 Tours, France
*E-mail address*: raschel@math.cnrs.fr