Asymptotic normality and greatest common divisors

José L. Fernández and Pablo Fernández

May 9, 2013

Abstract

We report on some statistical regularity properties of greatest common divisors: for large random samples of integers, the number of coprime pairs and the average of the gcd’s of those pairs are approximately normal, while the maximum of those gcd’s (appropriately normalized) follows approximately a Fréchet distribution approximately. We also consider \( r \)-tuples instead of pairs, and moments other than the average.

1 Introduction

In this paper we report on some statistical regularities of the greatest common divisors of random pairs, or more generally, \( r \)-tuples, drawn from large samples of integers.

For any given integer \( n \geq 1 \), let us denote by \( X_1^{(n)}, X_2^{(n)}, \ldots \) a sequence of independent random variables uniformly distributed in \( \{1, \ldots, n\} \) and defined on a certain given probability space endowed with a probability \( P \).

The distribution of \( \gcd(X_1^{(n)}, X_2^{(n)}) \), the gcd of a random pair, is given by

\[
P(\gcd(X_1^{(n)}, X_2^{(n)}) = k) = \frac{1}{n^2} \sum_{j \leq n/k} \mu(j) \left\lfloor \frac{n}{jk} \right\rfloor^2,
\]

for \( 1 \leq k \leq n \). Asymptotically, as \( n \to \infty \), one has

\[
\lim_{n \to \infty} P(\gcd(X_1^{(n)}, X_2^{(n)}) = k) = \frac{1}{\zeta(2)} \frac{1}{k^2},
\]

which, in particular, for \( k = 1 \), is the classical result of Dirichlet (see, for instance, [17], Theorem 332) that

\[
\lim_{n \to \infty} P(\gcd(X_1^{(n)}, X_2^{(n)}) = 1) = \frac{1}{\zeta(2)}.
\]

For the mean and the variance of \( \gcd(X_1^{(n)}, X_2^{(n)}) \) one has the asymptotic results

\[
\mathbb{E}(\gcd(X_1^{(n)}, X_2^{(n)})) \sim \frac{1}{\zeta(2)} \ln(n) \quad \text{and} \quad \mathbb{V}(\gcd(X_1^{(n)}, X_2^{(n)})) \sim \left[ \frac{1}{3} \left( \frac{2\zeta(2)}{\zeta(3)} - 1 \right) \right] n.
\]

as \( n \to \infty \). We refer to E. Cesàro [5], E. Cohen [8], and P. Diaconis and P. Erdős [12] for some further details and references. See also Section 3 of this paper.

\begin{footnotesize}
\begin{center}
\textbf{2010 Mathematics Subject Classification:} 60F05, 62E20, 11N37, 62H10.
\end{center}
\end{footnotesize}

Keywords: Gcd, asymptotic normality, U-statistics, locally dependent random variables, Euler, Jordan and Pillai functions, strong law.
Fix $n \geq 1$. For each integer $m \geq 2$, consider the random variable

$$C_m^{(n)} = \sum_{1 \leq i < j \leq m} 1_{\gcd(X_i^{(n)}, X_j^{(n)}) = 1},$$

which counts the number of coprime pairs in a random sample of length $m$ drawn from $\{1, \ldots, n\}$. Observe that $C_m^{(n)}$ does not exceed $\binom{m}{2}$ and attains that maximum value precisely when the whole sample $(X_1^{(n)}, X_2^{(n)}, \ldots, X_m^{(n)})$ is pairwise coprime. The formula

$$\lim_{n \to \infty} P\left((X_1^{(n)}, \ldots, X_m^{(n)}) \text{ pairwise coprime}\right) = \lim_{n \to \infty} P\left(C_m^{(n)} = \frac{m}{2}\right)$$

$$= \prod_p \left(\left(1 - \frac{1}{p}\right)^{m-1}(1 + \frac{m-1}{p})\right) := T_m$$

was proved by L. Toth, [30], and also by J. Cai and E. Bach, [4]. In the case $m = 2$, this limit probability reduces to the classical result of Dirichlet mentioned above, $T_2 = 1/\zeta(2)$.

As the size $m$ of the sample tends to $\infty$, the probability $T_m$ of pairwise coprimality tends to 0, see [30], and also [21]. This is to be compared with the extension of Dirichlet’s Theorem, see Section 2 for references, that for each $m \geq 2$,

$$\lim_{n \to \infty} P\left((X_1^{(n)}, \ldots, X_m^{(n)}) \text{ coprime}\right) = \lim_{n \to \infty} P\left(\gcd(X_1^{(n)}, \ldots, X_m^{(n)}) = 1\right) = \frac{1}{\zeta(m)}.$$

Now, the probability $1/\zeta(m)$ of just (mutual) coprimality tends to 1, as the sample size $m$ tends to $\infty$.

The exact distribution of $C_m^{(n)}$, for sample size $m$ given and $n$ fixed, is combinatorially involved; see J. Hu, [20], for an interesting approach.

In this paper we prove that $C_m^{(n)}$ is asymptotically normal as $m$ tends to $\infty$ when $n$ is fixed and, more generally, when $n$ is allowed to vary with $m$, with the only restriction that $n \geq 2$.

**Theorem A.** For each fixed $n \geq 2$,

$$\frac{C_m^{(n)} - \mathbb{E}(C_m^{(n)})}{\sqrt{\text{Var}(C_m^{(n)})}} \xrightarrow{d} \mathcal{N}, \quad \text{as} \ m \to \infty.$$  

More generally, the conclusion holds with $n$ replaced by any sequence $n_m$ of integers $n_m \geq 2$.

(This is Theorem 4.3 in Section 4). By $\xrightarrow{d}$ we mean convergence in distribution; $\mathcal{N}$ represents a standard normal variable.

The counter $C_m^{(n)}$ is a sum of $\binom{m}{2}$ Bernoulli variables with common probability of success, but, of course, they are not independent.

The analysis of $C_m^{(n)}$ could be framed into, at least, two different approaches. On the one hand, for fixed $n$, we could consider $C_m^{(n)}$, or rather $C_m^{(n)}/\binom{m}{2}$, as a sequence of $U$-statistics associated to the symmetric kernel $\gcd(x, y)$ and apply some general asymptotic results of W. Hoeffding, [19]. Alternatively, we could consider the collection of random variables $\gcd(X_i^{(n)}, X_j^{(n)})$, $1 \leq i < j \leq m$, as a family of locally dependent and identically distributed variables, and apply some general limit theorems for the sum of such a family, like those of S. Janson, [16], or P. Baldi and Y. Rinnoy, [1] and [2]. This second approach appears to be more flexible, particularly when $n$ is allowed to vary with $m$; it is the one we shall follow.

Both approaches depend on appropriate estimates of covariances of pairs of variables $\left(1_{\gcd(X_i^{(n)}, X_j^{(n)}) = 1}, 1_{\gcd(X_k^{(n)}, X_l^{(n)}) = 1}\right)$, of number theoretical nature, which we discuss in Sections 2 and 3.
We also consider some other natural $U$-statistics like the sum of gcd of pairs from the sample,
\[
Z_m^{(n)} = \sum_{1 \leq i < j \leq m} \gcd(X_i^{(n)}, X_j^{(n)}),
\]
instead of counting coprime pairs. We have:

**Theorem B.** For each fixed $n \geq 2$,
\[
\frac{Z_m^{(n)} - \mathbb{E}(Z_m^{(n)})}{\sqrt{\mathbb{V}(Z_m^{(n)})}} \xrightarrow{d} \mathcal{N}, \quad \text{as } m \to \infty.
\]
More generally, the conclusion holds with $n$ replaced by any sequence $n_m$ of integers $n_m \geq 2$ which verify $n_m \leq m^\beta$, for $\beta < 1/2$.

(This is Theorem 4.8 in Section 4). Notice that, in contrast to Theorem A, it is now required that the size of the sample space $n_m$ does not grow too fast as compared with the sample size $m$. It would be interesting to know whether this is really necessary and not just a restriction of the method of proof.

We consider also, in the opposite end, the random variables
\[
\mathcal{M}_m^{(n)} = \max_{1 \leq i < j \leq m} \{ \gcd(X_i^{(n)}, X_j^{(n)}) \},
\]
or, rather, their normalized version $\tilde{\mathcal{M}}_m^{(n)} = (\binom{m}{2})^{-1} \mathcal{M}_m^{(n)}$. In [9], Darling and Pyle obtained some interesting asymptotic results about $\tilde{\mathcal{M}}_m^{(n)}$, and asked whether it has a limit, in distribution, as $m \to \infty$. That this is the case is the content of:

**Theorem C.** Let $m^\beta \leq n \leq e^{n^\gamma}$, for some $\beta > 2$ and $\gamma < 1/3$. Then, for any $t > 0$,
\[
\lim_{m \to \infty} \mathbb{P}(\tilde{\mathcal{M}}_m^{(n)} \leq t) = \exp \left( -\frac{1}{\zeta(2)} t \right),
\]
so that $\tilde{\mathcal{M}}_m^{(n)}$ tends, in distribution, as $m \to \infty$, to the Fréchet distribution with shape parameter 1 and scale parameter $1/\zeta(2)$.

(This is Theorem 4.10 in Section 4). Our derivation of Theorem C is based on a classical result of Brown and Silverman (see [3], [29]) on Poisson approximation of $U$-statistics.

These theorems, A, B, and C, have corresponding counterparts for gcd of $r$-tuples, instead of just pairs, or for higher moments of gcd instead of just first moments, which we discuss in Sections 5 and 6.

The paper is organized as follows. Section 2 contains results about Euler’s $\varphi$ and Pillai’s $P$ function which are needed later. Section 3 derives some estimates of marginal probabilities and expectations, and of the appropriate covariances. Section 4 contains the proofs of Theorems A, B, and C. Section 5 considers the extension of those results to $r$-tuples, while Section 6 discusses the extension to higher moments. Finally, Section 7 discusses a strong law for gcd.

**Some notation:**

At a number of places we shall have products indexed by prime numbers: $\prod_p$ means product running over all primes $p$, while $\prod_{p \leq k}, \prod_{p \mid k}$ are products running over primes which are less than or equal to $k$, and over primes which divide $k$, respectively.

We denote by $I_s$ the arithmetic function $I_s(j) = j^s$ and simply write $I$ for $I_1$. With $\delta_k$ we denote the arithmetic function $\delta_k(j) = 1$ if $j = k$, and $\delta_k(j) = 0$ otherwise. The number of divisors of an integer $j \geq 1$ is denoted by $\tau(j)$. For any positive real number $x$, we denote by $\{x\}$ its fractional part: $\{x\} = x - \lfloor x \rfloor$. The Möbius function is $\mu$, and $*$ denotes Dirichlet convolution. For two sequences of positive numbers $(a_n)$ and $(b_n)$, by $a_n \sim b_n$ as $n \to \infty$, we mean that $\lim_{n \to \infty} a_n/b_n = 1$. 

3
2 Euler’s $\varphi$, Pillai’s $P$ function, and extensions

We collect in this section a number of identities and estimates involving Euler’s $\varphi$ function, Pillai’s $P$ function, and their corresponding $s$-dimensional versions $\varphi_s$ (Jordan’s totient functions) and $P_s$.

2.1 Euler’s and Jordan’s function

Euler’s $\varphi$ function,

$$\varphi(k) = \sum_{j=1}^{k} 1_{\gcd(j,k)=1}, \text{ for each } k \geq 1,$$

satisfies the identity $\varphi = \mu \ast I$, and verifies that

$$\frac{\varphi(k)}{k} = \prod_{p|k} \left(1 - \frac{1}{p}\right), \text{ for each } k \geq 1.$$

Observe that $\varphi(k) \leq k$, for every integer $k \geq 1$.

2.1.1 A double series involving $\varphi$ and $\gcd$

For every $t > 1$, define

$$(2.1) \quad M(t) := \sum_{i,j=1}^{\infty} \frac{\varphi(i)}{i} \frac{\varphi(j)}{j} \gcd(i,j).$$

The following identity shall prove useful:

**Lemma 2.1.** For every $t > 1$,

$$(2.2) \quad M(t) = \zeta(2t-1) \prod_p \left(1 + \frac{2}{p^t} - \frac{2}{p^{t+1}} - \frac{1}{p^{2t+1}} \right)$$

$$= \zeta(2t-1)\zeta(t)^2 \prod_p \left(1 - \frac{2}{p^{t+1}} - \frac{3}{p^{2t}} + \frac{3}{p^{2t+1}} + \frac{2}{p^{3t}} - \frac{1}{p^{4t+1}} \right).$$

Observe, in particular, that $M(t) < +\infty$ for every $t > 1$. The second product expression for $M(t)$ in (2.2) will be most convenient so as to apply some Tauberian theorem, see Corollary 2.2.

The proof of Lemma 2.1 uses the so-called zeta (probability) distributions on $\mathbb{N}$: for each real $t > 1$, the zeta distribution $\mathcal{Q}_t$ on $\mathbb{N}$ is given by

$$\mathcal{Q}_t(j) = \frac{1}{\zeta(t)^j}, \text{ for each integer } j \geq 1.$$}

For every prime number $p$, the random variable $\alpha_p$ on $\mathbb{N}$ assigns to each integer $j \geq 1$ the largest exponent $\alpha \geq 0$ so that $p^\alpha | j$ (thus $p^{\alpha_p(j)} | j$, but $p^{\alpha_p(j)+1} \nmid j$); in particular, $\{\alpha_p > 0\}$ is the event “divisible by $p$”, and, besides,

$$j = \prod_p p^{\alpha_p(j)}, \text{ for each integer } j \geq 1.$$

With respect to $\mathcal{Q}_t$, the variables $\{\alpha_p\}_p$ are mutually independent, and, moreover, each $\alpha_p$ is distributed as a geometric random variable on $\{0, 1, 2, \ldots\}$ with success probability $1 - 1/p^t$:

$$\mathcal{Q}_t(\alpha_p = k) = \left(1 - \frac{1}{p^t}\right) \frac{1}{p^k}, \text{ for each integer } k \geq 0.$$
Proof of Lemma 2.1. We first observe that the second infinite product expression follows from the first one and the Euler product expansion for \( \zeta(t) = \prod_p \frac{1}{1 - \frac{1}{p^t}} \); so that we just verify the first one.

We denote by \( Q_t^2 \) the product probability \( Q_t^2 \times Q_t^2 \) on \( \mathbb{N}^2 \) and write \( E_{Q_t^2} \) for the corresponding expectations. Consider the variable \( G \) on \( \mathbb{N}^2 \) given by

\[
(i, j) \in \mathbb{N}^2 \mapsto G(i, j) = \frac{\varphi(i)}{i} \frac{\varphi(j)}{j} \gcd(i, j).
\]

Observe that, for \( t > 1 \),

\[
E_{Q_t^2}(G) = \frac{1}{\zeta(t)^2} \sum_{i, j = 1}^{\infty} \frac{\varphi(i) \varphi(j)}{i^{1+t} j^{1+t}} \gcd(i, j).
\]

We introduce the auxiliary arithmetic function \( h \) given by \( h(j) = 1 \), if \( j \geq 1 \), and \( h(0) = 0 \), so that we may write \( \varphi \) and \( \gcd \) in terms of the variables \( \alpha_p \) as

\[
\frac{\varphi(j)}{j} = \prod_{p \mid j} \left( 1 - \frac{1}{p} \right) = \prod_p \left( 1 - \frac{h(\alpha_p(j))}{p} \right) \quad \text{and} \quad \gcd(i, j) = \prod_p p^{\min(\alpha_p(i), \alpha_p(j))},
\]

and then \( G \) itself as

\[
G(i, j) = \prod_p \left( 1 - \frac{h(\alpha_p(i))}{p} \right) \left( 1 - \frac{h(\alpha_p(j))}{p} \right) p^{\min(\alpha_p(i), \alpha_p(j))},
\]

which is an infinite product of mutually independent random variables.

Now, for each fixed prime \( p \), we have that

\[
E_{Q_t^2} \left[ \left( 1 - \frac{h(\alpha_p(i))}{p} \right) \left( 1 - \frac{h(\alpha_p(j))}{p} \right) p^{\min(\alpha_p(i), \alpha_p(j))} \right]
= \sum_{k, l = 0}^{\infty} \left( 1 - \frac{h(k)}{p} \right) \left( 1 - \frac{h(l)}{p} \right) p^{\min(k, l)} \left( 1 - \frac{1}{p^t} \right)^2 \frac{1}{p^{tk}} \frac{1}{p^{tl}}.
\]

Split the range of the double sum into \( \{ k = 0, l = 0 \} \), \( \{ k = 0, l > 0 \} \), \( \{ k > 0, l = 0 \} \) and \( \{ k > 0, l > 0 \} \), sum several geometric series and simplify to get the compact expression:

\[
E_{Q_t^2} \left[ \left( 1 - \frac{h(\alpha_p(i))}{p} \right) \left( 1 - \frac{h(\alpha_p(j))}{p} \right) p^{\min(\alpha_p(i), \alpha_p(j))} \right]
= \frac{(1 - 1/p^t)^2}{(1 - 1/p^{2t+1})} \left( 1 + \frac{2}{p^t} - \frac{2}{p^{t+1}} - \frac{1}{p^{2t+1}} \right).
\]

Now, since the \( \alpha_p \)'s are mutually independent, we may write, at least formally, that

\[
E_{Q_t^2}(G) = \frac{\zeta(2t - 1)}{\zeta(t)^2} \prod_p \left( 1 + \frac{2}{p^t} - \frac{2}{p^{t+1}} - \frac{1}{p^{2t+1}} \right),
\]

to obtain the desired result.

To justify the formal step, denote \( H(i, j) = \gcd(i, j) = \prod_p p^{\min(\alpha_p(i), \alpha_p(j))} \). Observe that

\[
E_{Q_t^2}(H) = \frac{1}{\zeta(t)^2} \sum_{i,j=1}^{\infty} \frac{\gcd(i, j)}{i^t j^t} = \frac{\zeta(2t - 1)}{\zeta(2t)} < +\infty.
\]
The last identity follows from the following elementary argument with the Möbius function: for any arithmetical function $f$

$$
\sum_{1 \leq x_1, \ldots, x_r \leq n \atop \gcd(x_1, \ldots, x_r) = 1} f(x_1, \ldots, x_r) = \sum_{k=1}^{n} \mu(k) \sum_{1 \leq x_1, \ldots, x_r \leq n \atop k \mid x_1, \ldots, x_r} f(x_1, \ldots, x_r)
$$

(2.3)

$$
= \sum_{k=1}^{n} \mu(k) \sum_{1 \leq y_1, \ldots, y_r \leq n/k} f(ky_1, \ldots, ky_r),
$$

Using (2.3), we can write

$$
\infty \sum_{i,j=1}^{\infty} \frac{\gcd(i,j)}{i^t j^t} = \sum_{d=1}^{\infty} d \sum_{d \mid \gcd(i,j)=d} \frac{1}{i^t j^t} = \sum_{d=1}^{\infty} \frac{1}{d^{2t-1}} \sum_{d \mid \gcd(a,b)=1} \frac{1}{a^t b^t}
$$

(2.4)

For every integer $N \geq 1$, define the partial product $G_N$ as

$$
G_N(i,j) = \prod_{p \leq N} \left(1 - \frac{h(\alpha_p(i))}{p}\right) \left(1 - \frac{h(\alpha_p(j))}{p}\right)^{\min(\alpha_p(i), \alpha_p(j))}
$$

Now, $G_N(i,j) \leq H(i,j)$, and $\lim_{N \to \infty} G_N(i,j) = G(i,j)$, for any integers $i, j \geq 1$ and so, by dominated convergence, we deduce

$$
\lim_{N \to \infty} \mathbb{E}_{\mathcal{Q}_t}^2(G_N) = \mathbb{E}_{\mathcal{Q}_t}^2(G).
$$

And, finally, since $G_N$ is a finite product of independent variables, we have

$$
\mathbb{E}_{\mathcal{Q}_t}^2(G_N) = \prod_{p \leq N} \frac{(1 - 1/p^t)^2}{(1 - 1/p^{2t-1})} \left(1 + \frac{2}{p^t} - \frac{2}{p^{t+1}} - \frac{1}{p^{2t+1}}\right)
$$

and the proof is completed.

The double sum which would correspond to $t = 1$ is infinite:

$$
\sum_{i,j=1}^{\infty} \frac{\varphi(i)}{i^2} \frac{\varphi(j)}{j^2} \frac{\gcd(i,j)}{\gcd(i,j)} = +\infty;
$$

the following corollary gives a suitable estimate for its rate of convergence to $\infty$.

**Corollary 2.2.** As $N \to \infty$,

$$
\sum_{i,j \leq N} \frac{\varphi(i)}{i^2} \frac{\varphi(j)}{j^2} \frac{\gcd(i,j)}{\gcd(i,j)} \sim \Delta \ln(N)^3,
$$

where $\Delta$ is the number

$$
\Delta = \frac{1}{12} \prod_p \left(1 - \frac{5}{p^2} + \frac{5}{p^3} - \frac{1}{p^5}\right) \approx 0.01186.
$$

(The summation above is over the set of integers $i, j \geq 1$ whose product $i \cdot j \leq N$.) In particular,

$$
\liminf_{N \to \infty} \frac{1}{\ln(N)^3} \sum_{\text{lcm}(i,j) \leq N} \frac{\varphi(i)}{i^2} \frac{\varphi(j)}{j^2} \frac{\gcd(i,j)}{\gcd(i,j)} \geq \Delta.
$$
In the proof of Corollary 2.2 we shall resort to (a particular case of) the powerful Delange’s Tauberian Theorem, which we may write as follows:

**Theorem 2.3** (Delange, [10], Théorème 1). Let \( A(z) := \sum_{k=1}^{\infty} a_k \frac{z^k}{k} \) be a Dirichlet series with nonnegative coefficients which has abscissa of convergence \( \rho > 0 \) and is holomorphic on the whole axis \( \Re(z) = \rho \) except at the point \( s = \rho \).

Assume that for two functions \( F(z) \) and \( G(z) \), holomorphic in \( \Re(z) \geq \rho \), and for some real \( \beta > 0 \) we have

\[
A(z) = \frac{F(z)}{(z-\rho)^\beta} + G(z), \quad \text{for} \quad \Re(z) > \rho,
\]

and \( F(\rho) \neq 0 \). Then, as \( n \to \infty \),

\[
\sum_{k=1}^{n} a_k \sim \frac{F(\rho)}{\rho F(\beta)} n^\beta \left( \ln(N) \right)^{\beta-1}.
\]

For non integer \( \beta \), the power \((z-\rho)^\beta\) in (2.5) means its principal branch.

**Proof of Corollary 2.2.** Observe first that the asymptotic comparison closing the statement of the corollary follows simply from the fact that \( \text{lcm}(i,j) \leq i \cdot j \).

Denote by \( B(z) \) the (holomorphic and nonvanishing for \( \Re(z) > 1/2 \)) function \( B(z) = \prod_p \left( 1 - \frac{2}{p^{z+1}} - \frac{3}{p^{2z}} + \frac{3}{p^{2z+1}} + \frac{2}{p^{3z}} - \frac{1}{p^{3z+1}} \right) \).

Notice that \( B(1) = \prod_p (1 - 5/p^2 + 5/p^3 - 1/p^5) = 12 \Delta \). Also, denote by \( C \) the entire function \( C(z) = (z-1)\zeta(z) \), for \( z \in \mathbb{C} \), and observe that \( C(1) = 1 \).

Extend the function \( M \) given in (2.1) to a holomorphic function in \( \Re(z) > 1 \):

\[
M(z) = \sum_{i,j=1}^{\infty} \frac{\varphi(i) \varphi(j)}{i^{1+z} j^{1+z}} \gcd(i,j) = \zeta(2z-1) \zeta(z)^2 B(z).
\]

For each integer \( k \geq 1 \), define the *positive* coefficient

\[
a_k = \sum_{i-j=k} \frac{\varphi(i) \varphi(j)}{i j \gcd(i,j)}
\]

to express \( M \) as a Dirichlet series

\[
M(z) = \sum_{k=1}^{\infty} \frac{a_k}{k^z}, \quad \Re(z) > 1.
\]

For \( \Re(z) > 1 \) we may write

\[
M(z) = \frac{1}{(z-1)^3} \left[ \frac{1}{2} C(2z-1) C(z)^2 B(z) \right].
\]

The function \( F(z) = \frac{1}{2} C(2z-1) C(z)^2 B(z) \) is holomorphic for \( \Re(z) > 1/2 \), and \( F(1) = B(1)/2 \). Delange’s Tauberian Theorem (with \( \rho = 1, \beta = 3, F \) as above and \( G \equiv 0 \)) gives then that

\[
\sum_{k=1}^{n} a_k \sim \frac{F(1)}{\Gamma(3)} n \ln(n)^2 = \frac{B(1)}{4} n \ln(n)^2, \quad \text{as} \quad n \to \infty.
\]
From summation by parts, we finally deduce that
\[ \sum_{k=1}^{n} \frac{a_k}{k} \sim B(1) \frac{\ln(n)^3}{12} = \Delta n \ln(n)^3, \quad \text{as } n \to \infty, \]
and, therefore, as desired, that
\[ \sum_{i,j \leq n} \frac{\varphi(i) \varphi(j)}{ij} \frac{\gcd(i, j)}{j^2} \sim \Delta n \ln(n)^3, \quad \text{as } n \to \infty. \quad \square \]

### 2.1.2 Jordan’s functions

For each integer \( s \geq 1 \), the \((s-) Jordan totient function\), denoted here by \( \varphi_s \), is given by the convolution
\[ \varphi_s = \mu * I_s. \]

For each integer \( k \geq 1 \), the function \( \varphi_s \) counts the number of \( s \)-tuples of integers \( (k_1, \ldots, k_s) \) with \( 1 \leq k_1, \ldots, k_s \leq k \), such that \( \gcd(k_1, \ldots, k_s, k) = 1 \). Of course, \( \varphi_1 = \varphi \). Observe that
\[ \varphi_s(k) = k^s \sum_{j \mid k} \frac{\mu(j)}{j^s} = k^s \prod_{p \mid k} \left( 1 - \frac{1}{p^s} \right), \quad \text{for each integer } k \geq 1. \]

Notice also that \( \varphi_s \) satisfies \( 1 \leq \varphi_s(k) \leq k^s \), for each integer \( k \geq 1 \).

For \( \varphi_s \) there is an identity analogous to that of Lemma 2.1 for \( \varphi \):

**Lemma 2.4.** For every real \( t > 1 \), and for each integer \( s \geq 1 \)
\[ \sum_{i,j=1}^{\infty} \varphi_s(i) \varphi_s(j) \frac{\gcd(i, j)}{ij} = \zeta(2t - 1) \zeta(t)^2. \]

\[ \prod_{p} \left( 1 - \frac{2}{pt+s} - \frac{1}{p^{2t}} - \frac{2}{p^{2t+s-1}} + \frac{2}{p^{2t+s}} + \frac{1}{p^{2t+2s-1}} + \frac{2}{p^{2t+2s}} - \frac{1}{p^{4t+2s-1}} \right). \]

And a corresponding estimate:

**Corollary 2.5.** For each integer \( s \geq 1 \)
\[ \lim_{N \to \infty} \frac{1}{\ln(N)^3} \sum_{\text{lcm}(i,j) \leq N} \frac{\varphi_s(i) \varphi_s(j)}{ij} \frac{\gcd(i, j)}{j^{s+1}} \geq \Delta_s, \]
where
\[ \Delta_s = \frac{1}{12} \prod_{p} \left( 1 - \frac{4}{p^{s+1}} - \frac{1}{p^2} + \frac{4}{p^{s+2}} + \frac{1}{p^{2s+1}} - \frac{1}{p^{2s+3}} \right). \]

Of course, the constant \( \Delta_1 \) coincides with the constant \( \Delta \) of Corollary 2.2. The proof of Lemma 2.4 proceeds along the same lines as that of Lemma 2.1, but using now the expression
\[ \frac{\varphi_s(k)}{k^s} = \prod_{p} \left( 1 - \frac{h_0(p)}{p^s} \right). \]
2.1.3 Asymptotic behavior of averages of $\varphi$ and of $\varphi_s$: Schur’s constants

The following lemma records the asymptotic behavior of certain averages of $\varphi$ and $\varphi_s$.

**Lemma 2.6 (Schur’s constants).** For every integers $s, l \geq 1$,

\begin{equation}
S_l^{(s)} := \lim_{n \to \infty} \frac{1}{n} \sum_{k=1}^{n} \left( \frac{\varphi_s(k)}{k^s} \right)^l = \prod_p \left( 1 - \frac{1}{p} \left[ 1 - \left( 1 - \frac{1}{p} \right)^l \right] \right).
\end{equation}

The case $s = 1$ corresponds to the Euler $\varphi$ function. The particular case $l = 1$ reads

\[ S_1^{(1)} = \prod_p \left( 1 - \frac{1}{p} \right)^{1/2} = \frac{1}{\zeta(2)}, \]

and it is a direct consequence of the identity

\[ \frac{1}{n} \sum_{k=1}^{n} \varphi(k) = \frac{1}{n} \sum_{k=1}^{n} \sum_{j \mid k} \mu(j) = \sum_{j=1}^{n} \mu(j) \left[ \left\lfloor \frac{n}{j} \right\rfloor \right]. \]

The case $l \geq 2$ is a result of Schur (see [22], page 58).

The results for $\varphi_s$, with $s \geq 2$, may be obtained following the approach of [22]. Again, observe that $S_l^{(s)} = 1/\zeta(s+1)$. Notice, for later use, that for any integers $s \geq 1$ and $l \geq 2$,

\begin{equation}
S_l^{(s)} > (S_1^{(s)})^l;
\end{equation}

strict inequality. Actually, in this paper, only the exponents $l = 1, 2$ are needed.

2.2 Pillai’s functions

The arithmetic function of Pillai is defined for integer $k \geq 1$ as

\[ P(k) = \sum_{j=1}^{k} \gcd(j, k). \]

Observe that $P(k)$ may be written as

\[ P(k) = \sum_{d \mid k} d \varphi\left( \frac{k}{d} \right) = (\varphi * I)(k), \]

so that

\[ \frac{P(k)}{k} = \sum_{d \mid k} \frac{\varphi(d)}{d}. \]

Consider next, for each integer $s \geq 1$, the arithmetic function $P_s$ given by the convolution $P_s = \varphi * I_s$; thus

\[ P_s(k) = \sum_{i=1}^{k} \gcd(i, k)^s. \]

Observe that

\begin{equation}
\frac{P_s(k)}{k^s} = \sum_{d \mid k} \frac{\varphi(d)}{d^s}. \end{equation}

The function $P_s$ may be written also as $P_s = \varphi_s * I$ and interpreted alternatively as

\[ P_s(k) = \sum_{i_1, i_2, \ldots, i_s=1}^{k} \gcd(i_1, i_2, \ldots, i_s, k). \]

Notice also that

\begin{equation}
\frac{P_s(k)}{k^s} \leq \left( \frac{P(k)}{k} \right)^s \leq \tau(k), \quad \text{for each integer } k \geq 1.
\end{equation}

We refer to [31] for further information on $P$ and $P_s$.

Although both $\varphi_s = \mu * I_s$ and $P_s = \varphi_s * I_s$ are well defined for real $s \geq 1$, we just consider the case $s$ integer.
2.2.1 Asymptotic behavior of averages of $P$ and $P_s$

We shall need the asymptotic behavior of averages, first and second moments, of $P$ and $P_s$.

Since $P = \mu * I * I$, the Dirichlet series, with variable $z$, of Pillai’s function is given by:

$$
\sum_{k=1}^{\infty} P(k) \frac{1}{k^z} = \frac{(z-1)^2}{\zeta(z)}, \quad \text{for } \Re(z) > 2.
$$

Writing

$$
\sum_{k=1}^{\infty} P(k) \frac{1}{k^z} = \frac{(z)^2}{\zeta(z+1)}, \quad \text{for } \Re(z) > 1,
$$

we deduce directly, say from Delange’s Theorem 2.3, that

$$
\frac{1}{n} \sum_{k=1}^{n} P(k) \sim \frac{1}{\zeta(2)} \ln(n), \quad \text{as } n \to \infty.
$$

For $s \geq 2$, we may write, using $P_s = \mu * I * I_s$, that

$$
\sum_{k=1}^{\infty} P_s(k) \frac{1}{k^z} \frac{1}{k^s} = \frac{(z)(z+s-1)}{\zeta(z+s)}, \quad \text{for } \Re(z) > 1,
$$

and, to deduce, as above, that

$$
\lim_{n \to \infty} \frac{1}{n} \sum_{k=1}^{n} P_s(k) \frac{1}{k^s} = \frac{\zeta(s)}{\zeta(s+1)}.
$$

Thus,

**Lemma 2.7.** As $n \to \infty$,

(2.12) $\frac{1}{n} \sum_{k=1}^{n} P(k) \sim \frac{1}{\zeta(2)} \ln(n),$

(2.13) $\frac{1}{n} \sum_{k=1}^{n} P_s(k) \frac{1}{k^s} \to \frac{\zeta(s)}{\zeta(s+1)}, \quad \text{for } s \geq 2.$

To obtain the asymptotic behavior of the averages of $P$ and $P_s$ for exponent $l = 2$, we proceed as follows. For $s \geq 1$, we may write

$$
\frac{1}{n} \sum_{k=1}^{n} \left( \frac{P_s(k)}{k^s} \right)^2 = \frac{1}{n} \sum_{k=1}^{n} \left( \sum_{j|k} \varphi(j) \frac{1}{j^s} \right)^2 = \frac{1}{n} \sum_{k=1}^{n} \sum_{i,j|k} \varphi(i) \varphi(j) \frac{1}{i^s} \frac{1}{j^s}.
$$

$$
= \sum_{1 \leq i,j \leq n} \varphi(i) \varphi(j) \left( \frac{1}{n} \left\lfloor \frac{n}{\text{lcm}(i,j)} \right\rfloor \right)
$$

For fixed integers $i, j \geq 1$, we have that

$$
\frac{1}{n} \left\lfloor \frac{n}{\text{lcm}(i,j)} \right\rfloor \leq \frac{1}{\text{lcm}(i,j)} = \frac{\gcd(i,j)}{ij},
$$

and also that

$$
\lim_{n \to \infty} \frac{1}{n} \left\lfloor \frac{n}{\text{lcm}(i,j)} \right\rfloor = \frac{\gcd(i,j)}{ij}.
$$
We split the argument into the two cases $s \geq 2$ and $s = 1$. For $s \geq 2$, Lemma 2.1 gives that
\[
\sum_{i,j=1}^{\infty} \frac{\varphi(i)}{i^{s+1}} \frac{\varphi(j)}{j^{s+1}} \gcd(i,j) < +\infty.
\]
and dominated convergence then gives that
\[
\lim_{n \to \infty} \frac{1}{n} \sum_{k=1}^{n} \left( \frac{P_s(k)}{k^s} \right)^2 = M(s).
\]
For the case $s = 1$, write
\[
\frac{1}{n} \sum_{k=1}^{n} \left( \frac{P(k)}{k} \right)^2 = \sum_{\text{lcm}(i,j) \leq n} \frac{\varphi(i) \varphi(j)}{i^2 j^2} \left( \frac{1}{n} \left\lfloor \frac{n}{\text{lcm}(i,j)} \right\rfloor \right).
\]
(Notice the range of summation.) Using that for any fixed integer $K \geq 2$, one has that $\lfloor x \rfloor \geq (1 - 1/K)x$, for any real $x \geq K$, we may bound
\[
\frac{1}{n} \sum_{k=1}^{n} \left( \frac{P(k)}{k} \right)^2 \geq \sum_{\text{lcm}(i,j) \leq \#} \frac{\varphi(i) \varphi(j)}{i^2 j^2} \gcd(i,j).
\]
Using now Corollary 2.2 we may conclude that
\[
\liminf_{n \to \infty} \frac{1}{\ln(n)^3} \frac{1}{n} \sum_{k=1}^{n} \left( \frac{P(k)}{k} \right)^2 \geq (1 - 1/K)\Delta.
\]
and, consequently,
\[
\liminf_{n \to \infty} \frac{1}{\ln(n)^3} \frac{1}{n} \sum_{k=1}^{n} \left( \frac{P(k)}{k} \right)^2 \geq \Delta.
\]
We record these results in the following:

**Lemma 2.8.** For $s = 1$,
\[
(2.14) \quad \liminf_{n \to \infty} \frac{1}{\ln(n)^3} \frac{1}{n} \sum_{k=1}^{n} \left( \frac{P(k)}{k} \right)^2 \geq \Delta,
\]
while, for $s \geq 2$,
\[
(2.15) \quad \lim_{n \to \infty} \frac{1}{n} \sum_{k=1}^{n} \left( \frac{P_s(k)}{k^s} \right)^2 = M(s).
\]

**Remark 2.9 (A theorem of L. Toth).** A result of L. Toth (see [31], Theorem A) gives a precise version of (2.14):
\[
\frac{1}{n} \sum_{k=1}^{n} \left( \frac{P(k)}{k} \right)^2 \sim \Delta_{\text{Toth}} \ln(n)^3, \quad \text{as } n \to \infty,
\]
where $\Delta_{\text{Toth}}$ is the constant: $\Delta_{\text{Toth}} = \frac{1}{\pi} \prod_p \left( 1 + \frac{1}{p} - \frac{4}{p(p+1)} \right)$. Since for each $p$
\[
\left( 1 + \frac{1}{p^2} - \frac{4}{p(p+1)} \right) \left( 1 - \frac{1}{p^2} \right) = \left( 1 - \frac{5}{p^2} + \frac{5}{p^3} - \frac{1}{p^5} \right),
\]
actually, $\Delta_{\text{Toth}} = 2\Delta$. 

11
Observe that, from the discussion above and Toth’s Theorem, one deduces that
\[
\sum_{\text{lcm}(i,j) \leq n} \frac{\varphi(i) \varphi(j)}{i^2 j^2} \gcd(i,j) \sim \Delta_{\text{Toth}} \ln(n)^3, \quad \text{as } n \to \infty,
\]
while, according to Corollary 2.2,
\[
\sum_{i,j \leq n} \frac{\varphi(i) \varphi(j)}{i^2 j^2} \gcd(i,j) \sim \Delta \ln(n)^3, \quad \text{as } n \to \infty.
\]

3 Marginal probabilities and expectations

The following lemma registers a couple of elementary but useful closed formulas for expectation of functions of greatest common divisor. We shall call them Cesàro’s formulas (see [5] and [6]):

**Lemma 3.1.** Let \( F \) be any arithmetic function.

a) (Cesàro’s formula) For any integers \( n, r \geq 1 \),

\[
\mathbb{E}(F(\gcd(X_1^{(n)}, \ldots, X_r^{(n)}))) = \frac{1}{n^r} \sum_{j=1}^{n} (\mu * F)(j) \left\lfloor \frac{n}{j} \right\rfloor^r.
\]

b) (Cesàro’s marginal formula) For any integers \( 1 \leq k \leq n \), and \( r \geq 1 \),

\[
\mathbb{E}(F(\gcd(X_1^{(n)}, \ldots, X_r^{(n)}, k))) = \frac{1}{n^r} \sum_{j|k} (\mu * F)(j) \left\lfloor \frac{n}{j} \right\rfloor^r.
\]

The expression (3.1) is valid also for \( r = 1 \), with the conventional understanding that \( \gcd(j) = j \), for any integer \( j \geq 1 \). On the left hand side (3.2) we have expectation marginal on \( X_{r+1} = k \), while on the right the sum extends only over divisors of \( k \).

**Proof.** They both follow from (2.3). For (3.2), the following observation is also needed: for each integer \( k \geq 1 \), define \( F_k \) as the arithmetic function \( F_k(j) = F(\gcd(j,k)) \). Then for any integer \( j \geq 1 \),

\[
(\mu * F_k)(j) = \begin{cases} (\mu * F)(j), & \text{if } j \mid k, \\ 0, & \text{if } j \nmid k. \end{cases}
\]

For a fixed integer \( k \geq 1 \), Cesàro’s formula with \( F = \delta_k \) reads

\[
\mathbb{P}(\gcd(X_1^{(n)}, \ldots, X_r^{(n)}) = k) = \frac{1}{n^r} \sum_{j|n/k} \mu(j) \left\lfloor \frac{n}{kj} \right\rfloor^r,
\]
from which one deduces the following asymptotic result, as \( n \to \infty \), for the probability distribution of the gcd of a random \( r \)-tuple:

\[
\lim_{n \to \infty} \mathbb{P}(\gcd(X_1^{(n)}, \ldots, X_r^{(n)}) = k) = \frac{1}{\zeta(r) k^r},
\]
which, for the case \( k = 1 \), reads

\[
\lim_{n \to \infty} \mathbb{P}((X_1^{(n)}, \ldots, X_r^{(n)}) \text{ coprime}) = \frac{1}{\zeta(r)}.
\]

The case \( r = 2 \) is Dirichlet’s Theorem. For \( r \geq 3 \), see Cesàro [6] (page 293), D. N. Lehmer [25] (Chapter V), and also [7], [18] or [27].

12
If we set $F = I$ in Cesàro’s formula (3.1) we obtain, since $\mu * I = \varphi$, that

$$
\mathbb{E}(\gcd(X_1^{(n)}, \ldots, X_r^{(n)})) = \frac{1}{n^r} \sum_{j=1}^{n} \varphi(j) \left\lfloor \frac{n}{j} \right\rfloor^r,
$$

from which the following asymptotic results for the expectation of the gcd of a random $r$-tuple are deduced: for $r \geq 3$,

$$
(3.4) \quad \lim_{n \to \infty} \mathbb{E}(\gcd(X_1^{(n)}, \ldots, X_r^{(n)})) = \sum_{j=1}^{\infty} \frac{\varphi(j)}{j^r} = \frac{\zeta(r-1)}{\zeta(r)},
$$

while for $r = 2$,

$$
(3.5) \quad \mathbb{E}(\gcd(X_1^{(n)}, X_2^{(n)})) \sim \frac{1}{\zeta(2)} \ln(n), \quad n \to \infty.
$$

For the second moments of gcd, which we shall need later on, we have (see for instance Theorem A’ in [14], and the references therein):

$$
(3.6) \quad \text{for } r \geq 4, \quad \lim_{n \to \infty} \mathbb{E}(\gcd(X_1^{(n)}, X_2^{(n)}, \ldots, X_r^{(n)})^2) = \frac{\zeta(r-2)}{\zeta(r)};
$$

$$
(3.7) \quad \text{for } r = 3, \quad \mathbb{E}(\gcd(X_1^{(n)}, X_2^{(n)}, X_3^{(n)})^2) \sim \frac{1}{\zeta(3)} \ln(n) \quad \text{as } n \to \infty;
$$

$$
(3.8) \quad \text{for } r = 2, \quad \mathbb{E}(\gcd(X_1^{(n)}, X_2^{(n)})^2) \sim \left[\frac{1}{3} \left(\frac{2\zeta(2)}{\zeta(3)} - 1\right)\right]n \quad \text{as } n \to \infty.
$$

Two particularly relevant cases of the marginal formula (3.2) are obtained by setting $F = \delta_1$ and $F = I$. They will appear quite often along this paper; specific notations are in order.

[Marginal probability] With $F = \delta_1$, we obtain, for $1 \leq k \leq n$

$$
(3.9) \quad U_1^{(n)}(k) := \mathbb{P}(\gcd(X_1^{(n)}, \ldots, X_i^{(n)}, k) = 1) = \frac{1}{n} \sum_{j \mid k} \mu(j) \left\lfloor \frac{n}{j} \right\rfloor^r.
$$

For $r = 1$, $U_1^{(n)}(k)$ is the proportion of numbers in $\{1, \ldots, n\}$ which are coprime with $k$, the familiar Legendre function.

[Marginal expectation] With $F = I$, we obtain, for $1 \leq k \leq n$,

$$
(3.10) \quad W_r^{(n)}(k) := \mathbb{E}(\gcd(X_1^{(n)}, \ldots, X_i^{(n)}, k)) = \frac{1}{n^r} \sum_{j \mid k} \varphi(j) \left\lfloor \frac{n}{j} \right\rfloor^r.
$$

### 3.1 Estimates and asymptotic behavior

In this section we record some estimates for the marginal probabilities $U_r^{(n)}(k)$ and expectations $W_r^{(n)}(k)$ that we shall need later on. Both estimates come about from comparing their respective expressions (3.9) and (3.10) with the analogous expressions that you get by removing the floor $[\ ]$, and which are quite more manageable as they do not contain $n$.

In this section, expectations and variances with respect to the uniform probability in $\{1, \ldots, n\}$ will be denoted by $\mathbb{E}_n$ and $\mathbb{V}_n$, respectively. Thus for a function (random variable) $f$ defined on $\{1, \ldots, n\}$, we have, for instance, $\mathbb{E}_n(f) = \frac{1}{n} \sum_{j=1}^{n} f(j)$. 

13
Lemma 3.2 (Estimates for marginal probabilities and expectations). For any integers \( n, r \geq 1 \) and any integer \( k \), with \( 1 \leq k \leq n \), we have that

\[
|U_r^{(n)}(k) - \sum_{j|k} \frac{\mu(j)}{j^r}| = |U_r^{(n)}(k) - \frac{\varphi_r(k)}{k^r}| \leq \frac{r \tau(k)}{n},
\]

(3.11)

\[
0 \leq \sum_{j|k} \frac{\varphi(j)}{j^r} - W_r^{(n)}(k) = \frac{P_r(k)}{k^r} - W_r^{(n)}(k) \leq \begin{cases} \frac{k}{n}, & \text{if } r = 1, \\ r \tau(k)/n, & \text{if } r \geq 2. \end{cases}
\]

(3.12)

These, of course, are standard bounds. See, for instance, D. H. Lehmer (Lemma 4 in [24]) or Toth (equation (7) in [30]) for the case \( r = 1 \) of (3.11).

**Proof.** We shall use that \( x^r - \lfloor x \rfloor^r \leq rx^{r-1} \), for any \( x > 0 \).

a) We may bound

\[
\left| \sum_{j|k} \frac{\mu(j)}{j^r} - U_r^{(n)}(k) \right| = \frac{1}{n^r} \left| \sum_{j|k} \mu(j) \left( \left( \frac{n}{j} \right)^r - \left\lfloor \frac{n}{j} \right\rfloor^r \right) \right| \leq \frac{n}{n} \sum_{j|k} \frac{1}{j^r} \leq \frac{r}{n} \sum_{j|k} 1 = \frac{r \tau(k)}{n}.
\]

b) The fact that \( W_r^{(n)}(k) \leq P_r(k)/k^r \) is immediate (see (2.10)). Finally,

\[
\sum_{j|k} \frac{\varphi(j)}{j^r} - W_r^{(n)}(k) = \frac{1}{n^r} \sum_{j|k} \varphi(j) \left( \left( \frac{n}{j} \right)^r - \left\lfloor \frac{n}{j} \right\rfloor^r \right) \leq \frac{r}{n} \sum_{j|k} \frac{\varphi(j)}{j^{r-1}}.
\]

For \( r = 1 \), we use that \( \sum_{j|k} \varphi(j) = k \), while, for \( r \geq 2 \), we use that \( \sum_{j|k} \varphi(j)/j^{r-1} \leq \sum_{j|k} \varphi(j)/j \leq \tau(k) \).

3.1.1 Asymptotic behavior of means

The average values of the marginal probabilities and expectations are, simply,

\[
\mu_r^{(n)} := E_n(U_r^{(n)}) = \frac{1}{n} \sum_{k=1}^{n} U_r^{(n)}(k) = \mathbb{P} \left( \gcd(X_1^{(n)}, \ldots, X_r^{(n)}, X_{r+1}^{(n)}) = 1 \right),
\]

\[
\nu_r^{(n)} := E_n(W_r^{(n)}) = \frac{1}{n} \sum_{k=1}^{n} W_r^{(n)}(k) = \mathbb{E} \left( \gcd(X_1^{(n)}, \ldots, X_r^{(n)}, X_{r+1}^{(n)}) \right).
\]

From equations (3.3), (3.4) and (3.5), we have:

**Lemma 3.3.** For each integer \( r \geq 1 \),

\[
\lim_{n \to \infty} \mu_r^{(n)} = \frac{1}{\zeta(r+1)}.
\]

For each integer \( r \geq 2 \),

\[
\lim_{n \to \infty} \nu_r^{(n)} = \frac{\zeta(r)}{\zeta(r+1)},
\]

while, for \( r = 1 \),

\[
\nu_1^{(n)} \sim \frac{1}{\zeta(2)} \ln(n)
\]

14
3.1.2 Asymptotic behavior of variances

We denote by \( c_r^{(n)} \) the variance of the marginal probability \( U_r^{(n)} \):

\[
c_r^{(n)} := \mathbb{V}_n(U_r^{(n)}) = \mathbb{E}_n(U_r^{(n)})^2 - \mathbb{E}_n(U_r^{(n)})^2 = \frac{1}{n} \sum_{k=1}^{n} U_r^{(n)}(k)^2 - \left( \frac{1}{n} \sum_{k=1}^{n} U_r^{(n)}(k) \right)^2.
\]

Observe that we may interpret \( c_r^{(n)} \) as the covariance

\[
c_r^{(n)} = \text{cov}(1_{\gcd(X_1^{(n)}, X_2^{(n)}, \ldots, X_r^{(n)}) = 1}, 1_{\gcd(X_1^{(n)}, X_r^{(n)}, X_{r+2}^{(n)}, \ldots, X_{2r+1}^{(n)}) = 1}),
\]

where each of the two gcd's involves \( r + 1 \) among the \( X_j^{(n)} \)'s variables, sharing exactly one of them, \( X_1^{(n)} \). This interpretation follows by conditioning on the value of the common variable \( X_1^{(n)} \).

Appealing to the estimate of Lemma 3.2, we may compare second moments as follows

\[
\left| \frac{1}{n} \sum_{k=1}^{n} U_r^{(n)}(k)^2 - \frac{1}{n} \sum_{k=1}^{n} \left( \frac{\varphi_r(k)}{k^r} \right)^2 \right| \leq \frac{1}{n} \sum_{k=1}^{n} \left| U_r^{(n)}(k) - \varphi_r(k) \frac{k^r}{k^r} \right| \leq \frac{1}{n} \sum_{k=1}^{n} \left( r \frac{\tau(k)}{n} \right)^2 \leq \frac{2r}{n^2} \sum_{k=1}^{n} \tau(k) \leq \frac{2r}{n} (1 + \ln(n)),
\]

where, besides, we have used that \( U_r^{(n)}(k) \leq 1 \), that \( \varphi_r(k) \leq k^r \) and also that \( \sum_{k=1}^{n} \tau(k) \leq n(1 + \ln(n)) \) (see for instance [17, Theorem 320]).

From this, and recalling the definition (2.8) of Schur’s constant \( S_2^{(r)} \), we deduce that

\[
\lim_{n \to \infty} \frac{1}{n} \sum_{k=1}^{n} U_r^{(n)}(k)^2 = S_2^{(r)},
\]

and, consequently, in conjunction with Lemma 3.3, and since \( S_2^{(1)} = 1/\zeta(r + 1) \),

**Lemma 3.4.** For any integer \( r \geq 1 \),

\[
\lim_{n \to \infty} c_r^{(n)} = \lim_{n \to \infty} \mathbb{V}_n(U_r^{(n)}) = S_2^{(r)} - (S_1^{(r)})^2.
\]

We point out for later use that \( \lim_{n \to \infty} c_r^{(n)} > 0 \).

The analysis of the variance of the marginal expectation is a bit more involved. We introduce the notation \( d_r^{(n)} \) for the variance of the marginal expectation \( W_r^{(n)} \):

\[
d_r^{(n)} := \mathbb{V}_n(W_r^{(n)}) = \mathbb{E}_n(W_r^{(n)})^2 - \mathbb{E}_n(W_r^{(n)})^2 = \frac{1}{n} \sum_{k=1}^{n} W_r^{(n)}(k)^2 - \left( \frac{1}{n} \sum_{k=1}^{n} W_r^{(n)}(k) \right)^2.
\]

Observe that we may interpret \( d_r^{(n)} \) as the covariance

\[
d_r^{(n)} = \text{cov}(\gcd(X_1^{(n)}, X_2^{(n)}, \ldots, X_r^{(n)}), \gcd(X_1^{(n)}, X_{r+2}^{(n)}, \ldots, X_{2r+1}^{(n)}));
\]

where, again, each of the two gcd’s involves \( r + 1 \) among the \( X_j^{(n)} \)'s variables, sharing exactly one of them, \( X_1^{(n)} \).
We compare second moments as follows:

\[
\left| \frac{1}{n} \sum_{k=1}^{n} W_r^{(m)}(k)^2 - \frac{1}{n} \sum_{k=1}^{n} \left( \frac{P_r(k)}{k^r} \right)^2 \right| \leq \frac{1}{n} \sum_{k=1}^{n} \left| W_r^{(m)}(k) - \frac{P_r(k)}{k^r} \right| \left| W_r^{(m)}(k) + \frac{P_r(k)}{k^r} \right| \\
\leq \frac{1}{n} \sum_{k=1}^{n} \left| W_r^{(m)}(k) - \frac{P_r(k)}{k^r} \right| (2 \tau(k)),
\]

where we have used that \( W_r^{(m)}(k) \leq \frac{P_r(k)}{k^r} \leq \tau(k) \) (see (2.11) and (3.12)).

Now, we appeal to Lemma 3.2. For \( r = 1 \), we obtain that

\[
(3.15) \quad \left| \frac{1}{n} \sum_{k=1}^{n} W_r^{(m)}(k)^2 - \frac{1}{n} \sum_{k=1}^{n} \left( \frac{P_r(k)}{k^r} \right)^2 \right| \leq \frac{2}{n^r} \sum_{k=1}^{n} k \tau(k) \leq \frac{1}{n} \sum_{k=1}^{n} \tau(k) \leq 2(1 + \ln(n)),
\]

where we have used that \( k \leq n \) and, once again, that \( \sum_{k=1}^{n} \tau(k) \leq n(1 + \ln(n)) \). Notice that for \( r = 1 \) the bound obtained does not converge to 0.

For \( r \geq 2 \), we have that

\[
(3.16) \quad \left| \frac{1}{n} \sum_{k=1}^{n} W_r^{(m)}(k)^2 - \frac{1}{n} \sum_{k=1}^{n} \left( \frac{P_r(k)}{k^r} \right)^2 \right| \leq \frac{2}{n^r} \sum_{k=1}^{n} r \tau(k) = \frac{2r}{n^2} \sum_{k=1}^{n} \tau(k)^2.
\]

This bound does converge to 0, as \( n \to \infty \); this may be seen by recalling that \( \tau(k) = O_\delta(k^\delta) \), for any \( \delta > 0 \) (see [17], Theorem 3.15), or more precisely, by appealing to Ramanujan’s asymptotic result that \( \sum_{k=1}^{n} \tau(k)^2 \sim \frac{1}{36}n(\ln(n))^3 \), as \( n \to \infty \) (see [17], second note on Chapter XVIII and the references therein). Incidentally, the bound \( \sum_{k=1}^{n} k \tau(k) \) of (3.15) behaves asymptotically as \( \frac{1}{2}n^2 \ln(n) \), as \( n \to \infty \), since \( \sum_{k=1}^{\infty} \frac{k \tau(k)}{k^r} = \zeta(z - 1)^2 \) for \( \Re(z) > 2 \). In any case, in what follows we just need that the bound in (3.15) is \( o(\ln(n))^3 \) and that the bound in (3.16) is \( o(1) \).

We keep splitting the discussion into the case \( r = 1 \) and the case \( r \geq 2 \). We start with the latter.

If \( r \geq 2 \), the bound in equation (3.16) converges to 0, as \( n \to \infty \). Moreover, in this case, Lemma 2.8 gives

\[
\lim_{n \to \infty} \frac{1}{n} \sum_{k=1}^{n} \left( \frac{P_r(k)}{k^r} \right)^2 = M(r).
\]

We conclude that also

\[
\lim_{n \to \infty} \frac{1}{n} \sum_{k=1}^{n} W_r^{(m)}(k)^2 = M(r),
\]

and, therefore, that

\[
\lim_{n \to \infty} \mathbb{V}_n(W_r^{(m)}) = M(r) - \left( \frac{\zeta(r)}{\zeta(r + 1)} \right)^2.
\]

Since

\[
\frac{\zeta(r)}{\zeta(r + 1)} = \sum_{j=1}^{\infty} \frac{\varphi(j)}{j^{r+1}},
\]

we may, finally, write this limiting variance in the following appealing form:

\[
\lim_{n \to \infty} \mathbb{V}_n(W_r^{(m)}) = \sum_{1 \leq i, j < \infty} \frac{\varphi(i)}{i^{r+1}} \frac{\varphi(j)}{j^{r+1}} (\gcd(i, j) - 1).
\]
Now we turn to the case \( r = 1 \). Notice that the bound in equation (3.15) is of the order \( \ln(n) \), while, by Toth’s Theorem, see Remark 2.9, the average \( \frac{1}{n} \sum_{k=1}^{n} (P(k)/k)^2 \) is of order \( \ln(n)^3 \). Therefore,

\[
\frac{1}{n} \sum_{k=1}^{n} W_k^{(n)}(k)^2 \sim \Delta_{\text{Toth}} \ln(n)^3.
\]

Finally, since

\[
\left( \frac{1}{n} \sum_{k=1}^{n} W_k^{(n)}(k) \right)^2 = \left( \nu_1^{(r)} \right)^2 \sim \frac{1}{\zeta(2)^2} \ln(n)^2,
\]

we conclude that

\[
V_n(W^{(n)}_1) \sim \Delta_{\text{Toth}} \ln(n)^3.
\]

We have proved:

**Lemma 3.5.** For any integer \( r \geq 2 \),

\[
\lim_{n \to \infty} d_r^{(n)} = \lim_{n \to \infty} V_n(W_r^{(n)}) = \sum_{1 \leq i, j < \infty} \frac{\varphi(i) \varphi(j)}{i^r+1 j^r+1} \left( \gcd(i,j) - 1 \right),
\]

while, for \( r = 1 \),

\[
d_1^{(n)} = V_n(W_1^{(n)}) \sim \Delta_{\text{Toth}} \ln(n)^3, \quad \text{as } n \to \infty.
\]

### 4 Statistics of gcd of pairs

Equipped with the estimates that we have gathered in the last two sections, in particular, Lemmas 3.3, 3.4 and 3.5, we are now ready to tackle the statistics of gcd of pairs of large sample of integers. We shall focus in the limiting behavior, as the sample size \( m \) tends to infinity, of the distribution of the following three basic statistics:

\[
\begin{align*}
C_m^{(n)} &= \sum_{1 \leq i < j \leq m} 1_{\gcd(X_i^{(n)}, X_j^{(n)}) = 1}, \\
Z_m^{(n)} &= \sum_{1 \leq i < j \leq m} \gcd(X_i^{(n)}, X_j^{(n)}), \\
M_m^{(n)} &= \max_{1 \leq i < j \leq m} \{ \gcd(X_i^{(n)}, X_j^{(n)}) \},
\end{align*}
\]

that counts the number of coprime pairs,

which sums the gcd of pairs of the sample, and

which gives the maximum gcd of the pairs of the sample.

We should remark that the asymptotic results of Section 3.1 that pertain to this section on pairs are those with \( r = 1 \) (and not \( r = 2 \)).

#### 4.1 Asymptotic distribution of the number of coprime couples

We start with the counter

\[
\begin{align*}
C_m^{(n)} &= \sum_{1 \leq i < j \leq m} 1_{\gcd(X_i^{(n)}, X_j^{(n)}) = 1}, \\
a \text{sum of } \binom{n}{2} \text{ random variables, identically distributed but not independent}.
\end{align*}
\]
The expectation of \( c_m^{(n)} \) is given by

\[
E(c_m^{(n)}) = \binom{m}{2} E(1_{\gcd(n, X_j^{(n)})=1}) = \binom{m}{2} \mu_1^{(n)}.
\]

Recall (Lemma 3.3) that, as \( n \to \infty \),

\[
E(1_{\gcd(n, X_j^{(n)})=1}) = \mu_1^{(n)} \to_{n \to \infty} \frac{1}{\zeta(2)}.
\]

Notice also that

\[
\mathbb{V}(1_{\gcd(n, X_j^{(n)})=1}) = \mu_1^{(n)}(1 - \mu_1^{(n)}).
\]

For the variance of \( c_m^{(n)} \) we have:

**Lemma 4.1.** The variance of the variable \( c_m^{(n)} \) is given by

\[
\mathbb{V}(c_m^{(n)}) = \binom{m}{2} \mu_1^{(n)} (1 - \mu_1^{(n)}) + m(m-1)(m-2) c_1^{(n)}.
\]

Recall that

\[
\lim_{n \to \infty} c_1^{(n)} = \lim_{n \to \infty} \mathbb{V}_n(U_1^{(n)}) = S_2^{(1)} - (S_1^{(1)})^2 > 0
\]

(see Lemma 3.4). Therefore, since \( c_1^{(n)} > 0 \) for each \( n \geq 2 \), we have that

\[
C_1 := \inf_{n \geq 2} c_1^{(n)} > 0.
\]

**Proof.** The variable \( c_m^{(n)} \) is a sum of \( \binom{m}{2} \) terms, so there will appear \( \binom{m}{2}^2 \) terms in the expansion of its variance in terms of covariances of pairs of summands:

- \( \binom{m}{2} \) individual variances \( \mathbb{V}(1_{\gcd(n, X_j^{(n)})=1}) = \mu_1^{(n)} (1 - \mu_1^{(n)}) \);
- \( m(m-1)(m-2) \) covariances of the type
  \[
  \text{cov}(1_{\gcd(n, X_j^{(n)})=1}, 1_{\gcd(n, X_j^{(n)})=1}) = \mathbb{V}_n(U_1^{(n)}) = c_1^{(n)},
  \]
  (with exactly one \( X_j^{(n)} \) in common);
- plus \( \binom{m}{2}(m-2) \) covariances of the type
  \[
  \text{cov}(1_{\gcd(n, X_j^{(n)})=1}, 1_{\gcd(n, X_j^{(n)})=1})
  \]
  (with no \( X_j^{(n)} \) in common). All these covariances are 0, because of the independence of the \( X_j^{(n)} \)'s.

Equation (4.2) follows. \( \square \)

Consider now the collection of \( \binom{m}{2} \) variables \( 1_{\gcd(n, X_j^{(n)})=1} \), with \( i < j \), as the vertices of a graph \( G_m^{(n)} \); there is an edge joining a pair of vertices \( 1_{\gcd(n, X_i^{(n)})=1} \) and \( 1_{\gcd(n, X_j^{(n)})=1} \) if the sets of indexes \( \{i, j\} \) and \( \{k, l\} \) have exactly one index in common. Thus \( G_m^{(n)} \) is the dependency graph of the variables \( \{1_{\gcd(n, X_j^{(n)})=1}\}_{1 \leq i < j \leq n} \).

We will now apply an asymptotic normality result of S. Janson [16], see also P. Baldi and Y. Rinnot ([1], particularly Proposition 5), concerning sums of (locally) dependent variables.
Theorem 4.2 (Janson, Theorem 2 in [16]). Suppose that, for each integer \( t \geq 1 \), we have a family \( \{Y_{i_1}, \ldots, Y_{i_{Nt}}\} \) of \( N_t \) bounded random variables, with almost sure common bound \( |Y_{ij}| \leq A_t \). Let \( M_t \) be the maximal degree of the dependency graph \( \Gamma_t \) of the family \( \{Y_{i_1}, \ldots, Y_{i_{Nt}}\} \). Denote
\[
S_t = \sum_{j=1}^{N_t} Y_{ij},
\]
and let \( \sigma_t^2 = \mathbb{V}(S_t) \). If there exists an integer \( h \geq 3 \) such that
\[
\left( \frac{N_t}{M_t} \right)^{1/h} \frac{M_t A_t}{\sigma_t} \to 0 \quad \text{as} \quad t \to \infty,
\]
then
\[
\frac{S_t - \mathbb{E}(S_t)}{\sigma_t} \xrightarrow{d} \mathcal{N}, \quad \text{as} \quad t \to \infty.
\]

For the families \( \{1_{\gcd(X_{ij}) = 1}\}_{1 \leq i < j \leq n} \) with dependency graphs \( \Gamma_m^{(n)} \), the corresponding parameters of Janson’s Theorem are: number of variables \( N = \binom{m}{2} \), maximal degree: \( M = 2(m-2) \), uniform bound on the variables \( A = 1 \), and
\[
\sigma^2 = \left( \frac{m}{2} \right) \mu_1^{(n)} (1 - \mu_1^{(n)}) + m(m-1)(m-2) c_1^{(n)}.
\]
Only in this last parameter the size \( n \) of the sample space intervenes, but actually, we may bound
\[
\sigma^2 \geq m(m-1)(m-2) C_1,
\]
where \( C_1 \) is given in (4.3), as long as \( n \geq 2 \). Now,
\[
\left( \frac{N}{M} \right)^{1/h} \frac{M \mathcal{A}}{\sigma} \leq \left( \frac{m}{2(m-2)} \right)^{1/h} \frac{2(m-2)}{\sqrt{m(m-1)(m-2)C_1}} \to 0, \quad \text{as} \quad m \to \infty,
\]
as long as the integer \( h \geq 3 \). Summarizing, we have proved:

Theorem 4.3. The counter of coprime pairs \( c_m^{(n)} \) is asymptotically normal:
\[
\frac{C_m^{(n)} - \mathbb{E}(c_m^{(n)})}{\sqrt{\mathbb{V}(c_m^{(n)})}} \xrightarrow{d} \mathcal{N}, \quad \text{as} \quad m \to \infty,
\]
for any fixed \( n \geq 2 \). More generally,
\[
\frac{C_m^{(n_m)} - \mathbb{E}(c_m^{(n_m)})}{\sqrt{\mathbb{V}(c_m^{(n_m)})}} \xrightarrow{d} \mathcal{N}, \quad \text{as} \quad m \to \infty,
\]
for any sequence \( n_m \) as long as \( n_m \geq 2 \), for each \( m \).

It is perhaps more natural to consider \( \tilde{C}_m^{(n)} = \binom{m}{2}^{-1} c_m^{(n)} \), the average number of coprime pairs in the sample of size \( m \). For fixed \( n \geq 2 \), we have as, \( m \to \infty \),
\[
\frac{\tilde{C}_m^{(n)} - \frac{1}{\zeta(2)}}{2 \sqrt{c_1^{(n)}/m}} \xrightarrow{d} \mathcal{N}.
\]
So, for large \( m \) (the sample size) and \( n \) (the size of the sample space),
\[
\tilde{C}_m^{(n)} \approx \mathcal{N} \left( \frac{1}{\zeta(2)}, \frac{2}{\sqrt{m}} \sqrt{S_2^{(1)}/\zeta(2)^2} \right).
\]
Remark 4.4. Notice that, for \( n \) fixed, the variance of \( C_m^{(n)} \) is of the order \( \binom{m}{2}^{3/2} \). This is to be compared with the variance of a sum of \( \binom{m}{2} \) identically distributed and pairwise independent Bernoulli variables, which is of the order \( \binom{m}{2} \), and with the variance of a sum of \( \binom{m}{2} \) identically distributed Bernoulli variables with constant positive correlation among them, which is of the order \( \binom{m}{2}^2 \).

Remark 4.5. As we have mentioned in the introduction, Theorem 4.3 could be derived in the \( n \) constant case from the classical results of W. Hoeffding on normal approximation of \( U \) statistics, [19], see also [28]. The approach through dependency graphs appears to be more flexible, particularly when \( n \) is allowed to vary. In any case, asymptotic normality of standard \( U \) statistics could be derived from the dependency graph approach, see Application C in [1].

Remark 4.6. There are good estimates for the rate of converge to normality for sums of locally dependent variables, for instance, [2], which could be applied to the variables \( C_m^{(n)} \).

4.2 Sums of greatest common divisor of pairs

We now deal with the random variable

\[
Z_m^{(n)} = \sum_{1 \leq i < j \leq m} \gcd(X_1^{(n)}(i), X_j^{(n)}).
\]

The mean of \( Z_m^{(n)} \) is given by

\[
E(Z_m^{(n)}) = \binom{m}{2} \nu_1^{(n)},
\]

where

\[
\nu_1^{(n)} = E(\gcd(X_1^{(n)}, X_2^{(n)})) = E(W_1^{(n)}) \sim \frac{1}{\zeta(2)} \ln(n), \quad \text{as } n \to \infty.
\]

Recall, see (3.8), that

\[
E(\gcd(X_1^{(n)}, X_2^{(n)})^2) \sim \left[ \frac{1}{3} \left( \frac{2\zeta(2)}{\zeta(3)} - 1 \right) \right] n,
\]

and consequently, that, also,

\[
V(\gcd(X_1^{(n)}, X_2^{(n)})) \sim \left[ \frac{1}{3} \left( \frac{2\zeta(2)}{\zeta(3)} - 1 \right) \right] n.
\]

For the variance of \( Z_m^{(n)} \), we have, with the same argument as in Lemma 4.1:

Lemma 4.7. The variance of the variable \( Z_m^{(n)} \) is given by

\[
V(Z_m^{(n)}) = \binom{m}{2} V(\gcd(X_1^{(n)}, X_2^{(n)}) + m(m-1)(m-2)d_1^{(n)}).
\]

This follows since

\[
\text{cov}(\gcd(X_1^{(n)}, X_2^{(n)}), \gcd(X_1^{(n)}, X_3^{(n)})) = d_1^{(n)}
\]

(see (3.14)). Recall from Lemma 3.5 that

\[
d_1^{(n)} \sim \Delta \ln(n)^3, \quad \text{as } n \to \infty.
\]

With all this, we can now prove:
**Theorem 4.8.** The sum of gcd of pairs, $Z_m^{(n)}$, satisfies
\[
\frac{Z_m^{(n)} - E(Z_m^{(n)})}{\sqrt{V(Z_m^{(n)})}} \xrightarrow{d} N, \quad \text{as } m \to \infty
\]
for any fixed $n \geq 2$. More generally,
\[
\frac{Z_m^{(n_m)} - E(Z_m^{(n_m)})}{\sqrt{V(Z_m^{(n_m)})}} \xrightarrow{d} N, \quad \text{as } m \to \infty
\]
for any sequence $n_m$ as long as $n_m \geq 2$ for each $m \geq 1$, and that $n_m = O(m^\beta)$ as $m \to \infty$, for some $\beta < \frac{1}{2}$.

**Proof.** We follow the argument of Theorem 4.3, the case of sums of indicators. The (dependency) graph $\Gamma_m^{(n)}$ is the same except that the vertices are now labeled by the variables $\gcd(X^{(n)}_i, X^{(n)}_j)$. The parameters pertaining Janson’s Theorem are now: number of vertices $N = \binom{m}{2}$, maximal degree $M = 2(m-2)$, bound on the variables $A = n = n_m$, and
\[
\sigma^2 = \left( \binom{m}{2} \right) \mathbb{V}(\gcd(X^{(n)}_1, X^{(n)}_2)) + m(m-1)(m-2) d_1^{(n)} \geq m(m-1)(m-2) d_1^{(n)}.
\]
Finally, for $h$ an integer so large that $\beta + 1/h \leq \frac{1}{2}$,
\[
\left( \frac{N}{M} \right)^{1/h} \frac{MA}{\sigma} \leq \left( \frac{m}{2(m-2)} \right)^{1/h} \frac{2(m-2)n_m}{\sqrt{m(m-1)(m-2)d_1^{(n)}}} \xrightarrow{m \to \infty} 0,
\]
since $n_m = O(m^\beta)$, and since $d_1^{(n)} \sim \Delta_{\text{Toth}} \ln(n)^3$ (see Lemma 3.5).

**Remark 4.9.** It would be interesting to determine whether a restriction on the rate of growth of the sample space size like $n_m < m^\beta$, with $\beta < 1/2$ which we have imposed is necessary for the asymptotic normality of $Z_m^{(n)}$, and if that is so, what is the optimal rate.

### 4.3 Extreme statistics of gcd of pairs

We now turn our attention to the random variable which registers the maximum of the greatest common divisors of pairs of the sample.

\[
\mathcal{M}_m^{(n)} = \max_{1 \leq i < j \leq m} \{ \gcd(X^{(n)}_i, X^{(n)}_j) \}.
\]

In [9], Darling and Pyle studied the asymptotic behavior of the distribution of this variable, obtained some interesting results and asked whether its normalized version
\[
\tilde{\mathcal{M}}_m^{(n)} = \left( \binom{m}{2} \right)^{-1} \mathcal{M}_m^{(n)}
\]
had a limit in distribution as $m \to \infty$ or not. The following theorem provides an answer

**Theorem 4.10.** Let $m^\beta \leq n \leq e^{m^\gamma}$, for some $\beta > 2$ and $\gamma < 1/3$. Then, for any $t > 0$,
\[
\lim_{m \to \infty} P\left( \tilde{\mathcal{M}}_m^{(n)} \leq t \right) = \exp\left( -\frac{1}{t\zeta(2)} \right).
\]

In other terms, $\tilde{\mathcal{M}}_m^{(n)}$ tends, in distribution, as $m \to \infty$, to the Fréchet distribution with shape parameter $1$ and scale parameter $1/\zeta(2)$. 

21
Observe that this convergence result requires that the size of the sampling space \( n \) tends to infinity along with \( m \), the sample size, in contrast to the asymptotic normality results for the variables \( C_m^{(n)} \) and \( Z_m^{(n)} \), where the size of the sampling space \( n \) played a relatively secondary role (see Sections 4.1 and 4.2). Fréchet distribution is one of the standard distributions used in Extreme Value Theory.

Theorem 4.10 is a direct, and standard, consequence of the following result above Poisson convergence:

**Theorem 4.11.** Let \( n \) be as in Theorem 4.10. Let \( t > 0 \) and consider the random variable

\[
N_m^{(n)}(t) = \# \left\{ 1 \leq i < j \leq m : \gcd(X_i^{(n)}, X_j^{(n)}) > t \left( \frac{m}{2} \right) \right\}.
\]

Then, for each fixed \( t > 0 \), the sequence \( \{N_m^{(n)}(t)\}_m \) converges in distribution to a Poisson variable of parameter \( \lambda = \frac{1}{\zeta(2)} \):

\[
N_m^{(n)}(t) \overset{d}{\to} \text{Poisson} \left( \frac{1}{\zeta(2)} \right) \quad \text{as} \quad m \to \infty.
\]

**Proof of Theorem 4.10.** Just observe that according to Theorem 4.11

\[
P(\tilde{M}_m^{(n)} > t) = P \left( \max_{1 \leq i < j \leq m} \gcd(X_i^{(n)}, X_j^{(n)}) > t \left( \frac{m}{2} \right) \right)
\]

\[
= P(N_m^{(n)}(t) > 0) \xrightarrow[\quad m \to \infty \quad]{} 1 - \exp \left( -\frac{1}{\zeta(2)} t \right).
\]

In the proof of Theorem 4.11, we will use results of Silverman and Brown (see Theorem A in [29]) and of Brown and Silverman (see Theorem A in [3]) about Poisson convergence of \( U \)-statistics, which, for the pairwise case we may write as follows:

**Theorem 4.12** (Brown–Silverman). Let \( Y_1, Y_2, \ldots, Y_M \) be iid random variables taking values on some space \( S \). Let \( g(x, y) \) be a symmetric function defined on \( S^2 \) and taking values 0 and 1. Denote by \( T \) the counter

\[
T = \sum_{1 \leq i < j \leq M} g(Y_i, Y_j)
\]

Let \( \lambda = E(T) \) and

\[
\rho = M^4 \text{cov}(g(Y_1, Y_2), g(Y_2, Y_3))
\]

Then

\[
|P(T = k) - P(\text{Poisson}(\lambda) = k)| \leq C \left( \frac{\lambda^2}{M} + \sqrt{\frac{\rho}{M}} \right) \quad \text{for each integer} \ k \geq 0,
\]

where \( C \) is some absolute constant.

**Proof of Theorem 4.11.** a) We shall require a simple estimate for the distribution function of the greatest common divisor of a random pair. The mass function of the gcd of a pair satisfies, (see, for instance, [12]), that, for \( 1 \leq j \leq n \),

\[
\left| P(\gcd(X_1^{(n)}, X_2^{(n)}) = j) - \frac{1}{j^2 \zeta(2)} \right| \leq 4 \left( \frac{1 + \ln(n/j)}{nj} \right) \leq 4 \left( \frac{1 + \ln(n)}{n} \right) \frac{1}{j}.
\]
We deduce that, for $0 \leq k \leq n$,

$$
(4.6) \quad \left| P(\gcd(X_1^{(n)}, X_2^{(n)}) > k) - \frac{1}{\zeta(2)} \sum_{j=1}^{n} \frac{1}{j^2} \right| \leq 4 \left(1 + \ln(n)\right)^2 / n,
$$

b) We will also need a convenient estimate of $E(\gcd(X_1^{(n)}, X_2^{(n)}) \cdot \gcd(X_2^{(n)}, X_3^{(n)}))$. Recall (see Lemma 3.5) that

$$
\text{cov}(\gcd(X_1^{(n)}, X_2^{(n)}) \cdot \gcd(X_2^{(n)}, X_3^{(n)})) = d_1^{(n)} \sim \Delta_{\text{Thue}} \ln(n)^3,
$$

and, consequently,

$$
(4.7) \quad E(\gcd(X_1^{(n)}, X_2^{(n)}) \cdot \gcd(X_2^{(n)}, X_3^{(n)})) = O(\ln(n)^3).
$$

Consider a sequence $n = n^m$ satisfying the conditions $m^\beta \leq n_m \leq e^{m^\gamma}$, for some $\beta > 2$ and $\gamma < 1/3$. Fix $t > 0$. To apply Theorem 4.12, we define the function

$$
g_m(x, y) = \mathbf{1}_{\gcd(x, y) > t(m)}(n)
$$

for $1 \leq x, y \leq n$, and the random variable

$$
T_m = \sum_{1 \leq i < j \leq m} g_m(X_i^{(n)}, X_j^{(n)}),
$$

which counts the number of random pairs with gcd bigger than $t(m)$.

Let us estimate the corresponding parameters $\lambda_m$ and $\rho_m$. First,

$$
\lambda_m = E(T_m) = \left(\frac{m}{2}\right) P(\gcd(X_1^{(n)}, X_2^{(n)}) > t(m))
$$

We have that $\lim_{m \to \infty} \lambda_m = 1/t^2$. To verify this, let $K = \left[t(m)\right]$, and bound, using the estimate (4.6):

$$
\lambda_m \leq \left(\frac{m}{2}\right) P(\gcd(X_1^{(n)}, X_2^{(n)}) > K) \leq \left(\frac{m}{2}\right) \left(\frac{1}{\zeta(2)} \sum_{j=K+1}^{n} \frac{1}{j^2}\right) + \left(\frac{m}{2}\right) 4 \left(1 + \ln(n)\right)^2 / n,
$$

to deduce, since $n_m \geq m^\beta$, with $\beta > 2$, that

$$
\limsup_{m \to \infty} \lambda_m \leq \frac{1}{\zeta(2)}.
$$

Using $K = \left[t(m)\right]$, one gets analogously that $\liminf_{m \to \infty} \lambda_m \geq 1/t^2$.

Next, using estimate (4.7), we may bound

$$
\rho_m = m^4 \text{cov} \left(1_{\gcd(X_1^{(n)}, X_2^{(n)}) > t(m)}, 1_{\gcd(X_1^{(n)}, X_3^{(n)}) > t(m)}\right)
$$

$$
\leq m^4 E(1_{\gcd(X_1^{(n)}, X_2^{(n)}) > t(m)} \cdot 1_{\gcd(X_1^{(n)}, X_3^{(n)}) > t(m)})
$$

$$
\leq m^4 \frac{1}{t^2(n)^2} E(\gcd(X_1^{(n)}, X_2^{(n)}) \cdot \gcd(X_2^{(n)}, X_3^{(n)})) = \frac{1}{t^2} O(\ln(n)^3).
$$

Reverting to the notation of the statement of the theorem, and on account of Theorem 4.12 of Brown and Silverman, this estimate of $\rho_m$ implies that

$$
|P(N_m^{(n)}(t) = k) - P(\text{Poisson}(\lambda_m) = k)| \leq C' \left(\frac{\lambda_m^2}{m} + \frac{\ln(n)^{3/2}}{t\sqrt{m}}\right) \leq C'' \left(\frac{\lambda_m^2}{m} + \frac{m^{3/2}}{t\sqrt{m}}\right),
$$

23
since \( n = n_m \leq e^{m^7} \). Finally, since \( \gamma < 1/3 \), this gives that
\[
\lim_{m \to \infty} P \left( N_m^{(n)}(t) = k \right) = P \left( \text{Poisson} \left( \frac{m}{\xi(t)} \right) = k \right)
\]
for any integer \( k \geq 0 \), as desired.

**Remark 4.13.** About the lower restriction on \( n_m \) in Theorem 4.11 there is not much to say, since just the statement of convergence requires that \( n_m / \binom{m}{2} \to +\infty \), but it would be nice to know what is the upper restriction required, if any.

From Theorem 4.10, we deduce as a corollary an asymptotic concentration result of Darling and Pyle, [9], Theorem 1:

**Corollary 4.14.** If \( n = n_m \) satisfies \( n \geq m^\beta \), for some \( \beta > 2 \) and, also, \( n \leq e^{m^\gamma} \); for some \( \gamma < 1/3 \), then, for any sequence \( \delta_m > 0 \) with \( \lim_{m \to \infty} \delta_m = 0 \), we have that
\[
\lim_{m \to \infty} P \left( m^2 \delta_m < \max_{1 \leq i < j \leq m} \gcd \left( X_i^{(n)}, X_j^{(n)} \right) < m^2 \frac{1}{\delta_m} \right) = 1.
\]

**Remark 4.15.** Notice that Darling and Pyle prove the above corollary for the sequence \( n_m = e^{\alpha m} \), where \( \alpha \) is any positive number; a sequence which is beyond the range of our Corollary 4.14. It would be interesting to determine the optimal rate of growth of \( n_m \) for the validity both of Theorem 4.10 and of Corollary 4.14.

5 \( U \)-statistics for greatest common divisors of \( r \)-tuples

We shall assume throughout this section that \( r \geq 3 \). We consider now \( U \)-statistics summing over the collection of subsets of size \( r \) of the random sample of length \( m \).

5.1 Number of relatively prime \( r \)-tuples

Let us start with the variable
\[
C_{m,r}^{(n)} = \sum_{1 \leq i_1 < \cdots < i_r \leq m} 1_{\gcd(X_{i_1}^{(n)}, \ldots, X_{i_r}^{(n)}) = 1},
\]
the sum of \( \binom{m}{r} \) terms counting the number of coprime \( r \)-tuples in a random sample of size \( m \) drawn uniformly from \( \{1, \ldots, n\} \).

We have:

**Theorem 5.1.** For fixed \( r \geq 3 \) and for any sequence \( n_m \geq 2 \),
\[
\frac{C_{m,r}^{(n_m)} - E(C_{m,r}^{(n_m)})}{\sqrt{V(C_{m,r}^{(n_m)})}} \xrightarrow{d} \mathcal{N} \quad \text{as } m \to \infty.
\]

The argument to prove Theorem 5.1 follows the same steps as the case of pairs; so that we shall only indicate some specific differences. The mean of \( C_{m,r}^{(n)} \) is given by
\[
E(C_{m,r}^{(n)}) = \binom{m}{r} P \left( \gcd(X_1^{(n)}, \ldots, X_r^{(n)}) = 1 \right) = \binom{m}{r} \mu_{r-1}^{(n)};
\]
recall, from Lemma 3.3, that \( \lim_{n \to \infty} \mu_{r-1}^{(n)} = \frac{1}{\xi(r)} \).
Observe that, with \( s, r \) the number of pairs of subsets of size \( r \) for each \( 0 \leq r \leq s \), the product of binomial coefficients in the summand of index \( s \) increases with \( s \), and, in particular, \( \gamma_{r,s}^{(n)} \geq 0 \), for \( 0 \leq s \leq r \).

In terms of these covariances, the variance of \( C_{m,r}^{(n)} \) may be written as

\[
\mathbb{V}(C_{m,r}^{(n)}) = \sum_{s=0}^{r} \binom{m}{s} \left( \frac{m-s}{r-s} \right) \left( \frac{m-r}{r-s} \right) \gamma_{r,s}^{(n)}.
\]

The product of binomial coefficients in the summand of index \( s \) of this expression counts the number of pairs of subsets of size \( r \) with intersection of size \( s \) drawn from \( \{1, 2, \ldots, m\} \). Observe that, with \( s, r \) fixed and as \( m \to \infty \),

\[
\left( \frac{m}{s} \right) \left( \frac{m-s}{r-s} \right) \left( \frac{m-r}{r-s} \right) \sim \frac{1}{s!(r-s)!} m^{2r-s}.
\]

We may trivially bound (just keeping the term \( s=1 \) in (5.3) and using that \( \gamma_{r,s}^{(n)} \geq 0 \),

\[
\mathbb{V}(C_{m,r}^{(n)}) \geq m \left( \frac{m-1}{r-1} \right) \left( \frac{m-r}{r-1} \right) \gamma_{r,1}^{(n)}.
\]

Recall, see Lemma 3.4, that \( \lim_{n \to \infty} \gamma_{r,1}^{(n)} = S_2^{(r-1)} - (S_1^{(r-1)})^2 \), a positive quantity.

**Proof of Theorem 5.1.** We shall apply again Janson’s Theorem 4.2. Consider the (dependency) graph with \( \binom{m}{r} \) vertices labeled with the variables \( 1_{\gcd(X_{i_1}, \ldots, X_{i_r})=1} \) for \( 1 \leq i_1 < i_2 < \cdots < i_r \leq n \), and with an edge joining two vertices if they have at least one index of their labels in common. We record now the appropriate parameters in order to apply Theorem 4.2: the number of vertices \( N = \binom{m}{r} \); the bound on the variables, \( A = 1 \), since the variables are just indicators; the maximal degree

\[
M = \binom{m}{r} - \binom{m-r}{r} - 1 \sim \frac{r}{(r-1)!} m^{r-1}, \quad \text{as } m \to \infty,
\]

and

\[
\sigma^2 \geq m \left( \frac{m-1}{r-1} \right) \left( \frac{m-r}{r-1} \right) \gamma_{r,1}^{(n)}.
\]

Fix any integer \( h \geq 3 \). For some constant \( C_{r,h} \), we have that

\[
\left( \frac{N}{M} \right)^{1/h} \frac{M A}{\sigma} \leq C_{r,h} \left( \frac{m^r}{m^{r-1}} \right)^{1/h} \frac{m^{r-1}}{m^{r-1/2}} \frac{1}{\gamma_{r,1}^{(n)}} = C_{r,h} \frac{m^{1/h}}{\sqrt{\gamma_{r,1}^{(n)}}},
\]

which converges to 0 as \( m \to \infty \), whatever the sequence \( n_m \geq 2 \). 

\[\square\]
5.2 Sums of greatest common divisors of \( r \)-tuples

For the variable

\[
Z_{m,r}^{(n)} = \sum_{1 \leq i_1 < \cdots < i_r \leq m} \gcd(X_{i_1}^{(n)}, \ldots, X_{i_r}^{(n)})
\]

which sums the greatest common divisors of all the \( r \)-tuples of a random sample of length \( m \) drawn for \( \{1, \ldots, n\} \), we have:

**Theorem 5.2.** For fixed \( r \geq 3 \) and for any sequence \( n_m \) of integers satisfying \( 2 \leq n_m \leq m^3 \), for some \( \beta < 1/2 \),

\[
\frac{Z_{m,r}^{(n_m)} - \mathbb{E}(Z_{m,r}^{(n_m)})}{\sqrt{V(Z_{m,r}^{(n_m)})}} \overset{d}{\to} \mathcal{N} \quad \text{as} \quad m \to \infty.
\]

The proof of Theorem 5.2 is a variation of the proof of Theorem 5.1. We just discuss a few of ingredients.

The mean of \( Z_{m,r}^{(n)} \) is given by

\[
\mathbb{E}(Z_{m,r}^{(n)}) = \binom{m}{r} \mathbb{E}(\gcd(X_1^{(n)}, \ldots, X_r^{(n)})) = \binom{m}{r} \nu_r^{(n)}
\]

Let us define, for \( 0 \leq s \leq r \),

\[
(5.5) \quad \omega_{r,s}^{(n)} = \text{cov}(\gcd(X_1^{(n)}, \ldots, X_s^{(n)}, X_{s+1}^{(n)}, \ldots, X_r^{(n)}), \gcd(X_1^{(n)}, \ldots, X_s^{(n)}, X_{r+1}^{(n)}, \ldots, X_{2r-s}^{(n)}))
\]

Notice that \( \omega_{r,1}^{(n)} = d_{r-1}^{(n)} \), see (3.14). Again, \( \omega_{r,0}^{(n)} = 0 \), because of the independence of the \( X_j^{(n)} \)'s. Again, from Cauchy–Schwarz,

\[
(5.6) \quad \omega_{r,s}^{(n)} \leq \omega_{r,r}^{(n)} = \mathbb{V}(\gcd(X_1^{(n)}, X_2^{(n)}, \ldots, X_r^{(n)}))
\]

for each \( 0 \leq s \leq r \). And again, \( 0 = \omega_{r,0}^{(n)} \leq \omega_{r,s}^{(n)} \leq \omega_{r,r}^{(n)} \) for \( 0 \leq s \leq r \).

The variance of \( Z_{m,r}^{(n)} \) may be written as

\[
\mathbb{V}(Z_{m,r}^{(n)}) = \sum_{s=0}^{r} \binom{m}{s} \binom{m-s}{r-s} \binom{m-r}{r-s} \omega_{r,s}^{(n)}(n),
\]

so that we may bound

\[
\mathbb{V}(Z_{m,r}^{(n)}) \geq m \binom{m-1}{r-1} \binom{m-r}{r-1} d_{r-1}^{(n)}
\]

Recall, see Lemma 3.5, that, for \( r \geq 3 \),

\[
\lim_{n \to \infty} d_{r-1}^{(n)} = \sum_{1 \leq i,j < \infty} \frac{\varphi(i)}{i^r} \frac{\varphi(j)}{j^r} (\gcd(i,j) - 1),
\]

which is a positive and finite (since \( r \geq 3 \)) quantity.

For the proof of Theorem 5.2, we just have to observe that the parameter \( A \) to apply in Janson’s Theorem is now \( A = n \), and this is why we require now the bound \( n_m \leq m^3 \), with \( \beta < 1/2 \).
Remark 5.3 (Extreme Statistics of the greatest common divisor of $r$-tuples). Fix $r \geq 3$. It would be interesting to determine, if there is any at all, the corresponding approximation result for the maximum of $\gcd$ for $r$-tuples.

Let us see why the approach which we have followed for the case of pairs breaks down for $r \geq 3$. Following that approach, one would fix $t > 0$, consider the counter

$$T_m = \sum_{1 \leq i_1 < i_2 < \cdots < i_r \leq n} 1_{\gcd(X_{i_1}^{(n)}, X_{i_2}^{(n)}, \ldots, X_{i_r}^{(n)}) > ts_m},$$

where $\{s_m\}_m$ is some appropriate sequence, and expect to obtain convergence in distribution of $T_m$ to a Poisson variable.

Now $E(T_m) = \binom{m}{r} \mathbb{P}(\gcd(X_1^{(n)}, X_2^{(n)}, \ldots, X_r^{(n)}) > ts_m)$ should converge to the parameter $\lambda_t$ defining the purported limiting Poisson distribution. The distribution of $\gcd$ of $r$-tuples satisfies, for $1 \leq j \leq n$, that

$$\left| \mathbb{P}(\gcd(X_1^{(n)}, X_2^{(n)}, \ldots, X_r^{(n)}) = j) - \frac{1}{\zeta(r)} \right| \leq C_r \frac{1}{nj^{r-1}},$$

see, for instance, [14], and therefore, for $1 \leq k \leq n$,

$$\left| \mathbb{P}(\gcd(X_1^{(n)}, X_2^{(n)}, \ldots, X_r^{(n)}) > k) - \frac{1}{\zeta(r)} \sum_{j=k+1}^{n} \frac{1}{j^{r-1}} \right| \leq C_r \frac{1}{nk^{r-2}}.$$ 

With the forced choice of $s_m = \binom{m}{r}^{1/(r-1)}$, and as long as $\frac{n}{m^{r/(r-1)}} \to \infty$, we have that

$$\binom{m}{r} \mathbb{P}(\gcd(X_1^{(n)}, X_2^{(n)}, \ldots, X_r^{(n)}) > ts_m) \to \frac{1}{r-1} \frac{1}{\zeta(r)} = \lambda_t.$$

The general result of Brown and Silverman (Theorem A of [3]) for Poisson convergence of $U$-statistics requires that

$$m^{2r-1} \text{cov}(1_{\gcd(X_1^{(n)}, X_2^{(n)}, \ldots, X_{r-1}^{(n)}, X_{r+1}^{(n)}) > ts_m}, 1_{\gcd(X_1^{(n)}, X_2^{(n)}, \ldots, X_{r-1}^{(n)}, X_{r+1}^{(n)}) > ts_m}) \to 0,$$

as $m \to \infty$. If we simply estimate, as we did in the case of pairs,

$$\text{cov}(1_{\gcd(X_1^{(n)}, X_2^{(n)}, \ldots, X_{r-1}^{(n)}, X_{r+1}^{(n)}) > ts_m}, 1_{\gcd(X_1^{(n)}, X_2^{(n)}, \ldots, X_{r-1}^{(n)}, X_{r+1}^{(n)}) > ts_m})$$

$$\leq \mathbb{P}(\gcd(X_1^{(n)}, X_2^{(n)}, \ldots, X_{r-1}^{(n)}, X_{r+1}^{(n)}) > ts_m, \gcd(X_1^{(n)}, X_2^{(n)}, \ldots, X_r^{(n)} > ts_m))$$

$$\leq \frac{1}{ts_m} \mathbb{E}(\gcd(X_1^{(n)}, X_2^{(n)}, \ldots, X_r^{(n)}) \cdot \gcd(X_1^{(n)}, X_2^{(n)}, \ldots, X_r^{(n)})).$$

we get nowhere, because the expectation above is obviously at least 1, and

$$\frac{m^{2r-1}}{s_m^{2r-1}} \approx \frac{m^{2r-1}}{m^{2r-1}},$$

which for $r = 2$ tends to 0 with $m$, but for $r \geq 3$, our present case, tends to $\infty$ with $m$.

To obtain an asymptotic approximation results for the maximum of $\gcd$ for $r$-tuples following the approach which we have followed one would need a better estimate, if possible, of

$$\text{cov}(1_{\gcd(X_1^{(n)}, X_2^{(n)}, \ldots, X_{r-1}^{(n)}, X_{r+1}^{(n)}) > ts_m}, 1_{\gcd(X_1^{(n)}, X_2^{(n)}, \ldots, X_{r-1}^{(n)}, X_{r+1}^{(n)}) > ts_m}).$$
6 Higher moments

Finally, we consider in this section $U$-statistics of moments, other than first, of gcd. We follow, of course, the general approach of previous sections, particularly, Section 5.2; we will just mention the few extra ingredients needed to obtain the corresponding results for higher moments.

We fix throughout this section the integer exponent $q \geq 1$ and the length $r$ for the evaluation of gcd’s, and consider

$$Z_m^{(n)} = \sum_{1 \leq i_1 < i_2 < \cdots < i_r \leq m} \gcd \left( X_{i_1}^{(n)}, X_{i_2}^{(n)}, \ldots, X_{i_r}^{(n)} \right)^q.$$

Observe that, departing from previous usage, we are not decorating $Z_m^{(n)}$ with the length $r$ (or the exponent $q$).

For $n$ fixed, $n \geq 2$, and as $m \to \infty$, we have asymptotic normality for $Z_m^{(n)}$. This follows exactly as in Section 5.2.

**Theorem 6.1.** Given a length $r \geq 2$ and an exponent $q \geq 1$, then for fixed $n \geq 2$

$$Z_m^{(n)} = \sum_{1 \leq i_1 < \cdots < i_r \leq m} \gcd \left( X_{i_1}^{(n)}, X_{i_2}^{(n)}, \ldots, X_{i_r}^{(n)} \right)^q$$

is asymptotically normal as $m \to \infty$.

For varying $n = n_m$, the general approach hinges on estimating (from below) the covariance

$$\omega^{(n)} = \text{cov} \left( \gcd \left( X_1^{(n)}, X_2^{(n)}, \ldots, X_r^{(n)} \right)^q, \gcd \left( X_1^{(n)}, X_{r+1}^{(n)}, \ldots, X_{2r-1}^{(n)} \right)^q \right)$$

(just one variable $X^{(n)}$ in common). Now, as $n \to \infty$,

$$\mathbb{E} \left( \gcd \left( X_1^{(n)}, X_2^{(n)}, \ldots, X_r^{(n)} \right)^q \right) \begin{cases} \rightarrow \frac{\zeta(r-q)}{\zeta(r)}, & \text{if } q \leq r-2, \\ \sim \ln(n)/\zeta(r), & \text{if } q = r-1, \\ \sim D_{r,q} \cdot n^{q-r+1}, & \text{if } q \geq r, \end{cases}$$

for some constant $D_{r,q}$ (see [14]).

Conditioning on the value of $X_1^{(n)}$ and using Cesàro’s marginal formula (3.2), we may write

$$\pi^{(n)} := \mathbb{E} \left( \gcd \left( X_1^{(n)}, X_2^{(n)}, \ldots, X_r^{(n)} \right)^q \cdot \gcd \left( X_1^{(n)}, X_{r+1}^{(n)}, \ldots, X_{2r-1}^{(n)} \right)^q \right)$$

$$= \frac{1}{n} \sum_{k=1}^{n} \left( \frac{1}{n^r - \sum_{j \neq k} \varphi_q(j) \left[ \frac{n}{j} \right]^{-r-1}} \right)^2.$$

We split the analysis of $\pi^{(n)}$ into the three cases above.

a) For $q \leq r - 2$, we first write

$$\pi^{(n)} = \frac{1}{n} \sum_{k=1}^{n} \frac{1}{n^{2(r-1)}} \sum_{i,j \mid k} \varphi_q(i) \varphi_q(j) \left[ \frac{n}{i} \right]^{-r-1} \left[ \frac{n}{j} \right]^{-r-1}$$

$$= \sum_{i,j \leq n} \varphi_q(i) \varphi_q(j) \left[ \frac{n}{i} \right]^{-r-1} \left[ \frac{n}{j} \right]^{-r-1} \frac{n}{\text{lcm}(i,j)} \frac{1}{n^{2(r-1)}},$$

and then bound

$$\pi^{(n)} \leq \sum_{i,j \leq n} \frac{\varphi_q(i) \varphi_q(j)}{i^{r} j^{r}} \gcd(i,j).$$
Since
\[
\sum_{i,j \leq n} \frac{\varphi_q(i)}{i^r} \frac{\varphi_q(j)}{j^r} \gcd(i, j) \leq \sum_{i,j \leq n} \frac{\gcd(i, j)}{i^r-j^r-q} \leq \sum_{i,j \geq 1} \frac{\gcd(i, j)}{i^r-j^r-q} = \frac{\zeta(r-q)^2\zeta(2(r-q)-1)^2}{\zeta(2(r-q))}
\]
(see (2.4)), we may conclude from dominated convergence that
\[
\lim_{n \to \infty} \pi^{(n)} = \sum_{i,j \leq n} \frac{\varphi_q(i)}{i^r} \frac{\varphi_q(j)}{j^r} \gcd(i, j).
\]

Also,
\[
\lim_{n \to \infty} \mathbb{E}(\gcd(X^{(n)}_1, X^{(n)}_2, \ldots, X^{(n)}_r)^q) = \frac{\zeta(r-q)}{\zeta(r)} = \sum_{j=1}^{\infty} \frac{\varphi_q(j)}{j^r}
\]
so that, finally, we have, in this case, \(q \leq n - 2\), that
\[
\lim_{n \to \infty} \omega^{(n)} = \sum_{i,j=1}^{\infty} \frac{\varphi_q(i)}{i^r} \frac{\varphi_q(j)}{j^r} (\gcd(i, j) - 1)
\]
This means that we have asymptotic normality as long as \(n^q_m \leq m^\beta\) for some \(\beta < 1/2\).

b) Case \(q = r - 1\). We shall get that \(\pi^{(n)}\) is at least of order \(\ln(n)^3\). To see this use (twice) that \([x] \geq x/2\), if \([x] \geq 1\), to bound \(\pi^{(n)}\) from below:
\[
\pi^{(n)} \geq \frac{1}{4} \sum_{k=1}^{n} \left(\sum_{j \mid k} \frac{\varphi_q(j)}{j^q}\right)^2 = \frac{1}{4} \sum_{i,j \leq n} \frac{\varphi_q(i)}{i^q} \frac{\varphi_q(j)}{j^q} \left(\frac{1}{n} \left| \frac{n}{\gcd(i,j)} \right| \right)
\]
\[
\geq \frac{1}{8} \sum_{\gcd(i,j) \leq n} \frac{\varphi_q(i)}{i^{q+1}} \frac{\varphi_q(j)}{j^{q+1}} \gcd(i,j).
\]
Appealing now to Corollary 2.5, we deduce that
\[
\liminf_{n \to \infty} \frac{\pi^{(n)}}{\ln(n)^3} \geq \frac{1}{8} \Delta_q
\]
and further that
\[
\liminf_{n \to \infty} \frac{\omega^{(n)}}{\ln(n)^3} \geq \frac{1}{8} \Delta_q
\]
since
\[
\pi^{(n)} - \omega^{(n)} \sim \left(\frac{1}{\zeta(2)}\right)^2 \ln(n)^2.
\]
The outcome of all this is again that we have asymptotic normality for \(Z_m^{(n)}\) as long as \(n^q_m \leq m^\beta\) for some \(\beta < 1/2\).

We stop and record the consequence of the analysis in these two cases a) and b).

**Theorem 6.2.** Given a length \(r \geq 2\) and an exponent \(q \geq 1\) with \(q \leq r - 1\), then for any sequence \(n_m\) satisfying \(2 \leq n_m\) and \(n^q_m \leq m^\beta\), with \(\beta < 1/2\),
\[
Z_m^{(n)} = \sum_{1 \leq i_1 < \ldots < i_r \leq m} \gcd(X^{(n)}_{i_1}, \ldots, X^{(n)}_{i_r})^q is asymptotically normal as \(m \to \infty\).
\]

c) Case \(q \geq r\). One would expect that both \(\pi^{(n)}\) and \(\omega^{(n)}\) would grow in this case as \(n^{2(q-r+1)}\). But we have not been able to ascertain that. Nonetheless, if that were the case, then one would have asymptotic normality as long as \(2 \leq n_m\) and \(n^q_m \leq m^\beta\) with \(\beta < 1/2\).
7 Strong law

The sequence of counters $c_{m,r}^{(n)}$ indexed by $m$, with sample space $\{1, \ldots, n\}$, $n \geq 2$ fixed, and length $r \geq 2$ fixed, do satisfy a strong law of large numbers as $m \to \infty$.

**Theorem 7.1.**

$$\lim_{m \to \infty} \frac{c_{m,r}^{(n)}}{\mathbb{E}(C_{m,r}^{(n)})} = 1 \quad \text{almost surely.}$$

In other terms, for almost all realizations of the complete sequence $x_1^{(n)}, x_2^{(n)}, \ldots$, the sequence $\{\frac{c_{m,r}^{(n)}}{\mathbb{E}(C_{m,r}^{(n)})}\}_{m}$, where each successive term is calculated using the values of the given realization $\{x_k^{(n)}\}_k$, converges to 1.

Since $\mathbb{E}(C_{m,r}^{(n)}) = \binom{m}{r}\mu_{r-1}^{(n)}$, we could also write

$$\lim_{m \to \infty} \frac{c_{m,r}^{(n)}}{\binom{m}{r}} = \mu_{r-1}^{(n)} \quad \text{almost surely.}$$

Recall that, as $n \to \infty$, the mean $\mu_{r-1}^{(n)}$ converges to $1/\zeta(r)$.

There are general strong laws for $U$-statistics which could be applied, but we prefer, given our previous estimates of variances and covariances of gcd’s, to derive Theorem 7.1 directly from the following (standard) lemma:

**Lemma 7.2.** Let $(Y_m)_m$ be an increasing sequence of positive random variables in a probability space, such that

1) $\mathbb{E}(Y_m)$ increases to infinity at a polynomial rate,

2) $\mathbb{V}(Y_m) \leq C \mathbb{E}(Y_m)^\delta$, for some $0 < \delta < 2$.

Then

$$\lim_{m \to \infty} \frac{Y_m}{\mathbb{E}(Y_m)} = 1 \quad \text{almost surely.}$$

By “increasing at a polynomial rate” we mean that $\mathbb{E}(Y_m) \sim Cm^\beta$, for some $\beta > 0$, as $m \to \infty$.

**Proof of Theorem 7.1.** Fix $n \geq 2$ and $r \geq 2$. Let us verify that $Y_m = c_{m,r}^{(n)}$ satisfies the hypothesis of Lemma 7.2. Obviously $0 \leq Y_m \leq Y_{m+1}$. Besides, $\mathbb{E}(Y_m) = \mathbb{E}(C_{m,r}^{(n)}) = \binom{m}{r}\mu_{r-1}^{(n)}$ grows at polynomial rate, with $\beta = r$.

Recall, from (5.3), that

$$\mathbb{V}(c_{m,r}^{(n)}) = \sum_{s=0}^{r} \binom{m}{s} \binom{m-s}{r-s} \binom{m-r}{r-s} \gamma_{r,s}^{(n)}.$$

Now, since $\gamma_{r,s}^{(n)} \leq \omega_{r,r}^{(n)}$, for $s$ from $s = 0$ to $s = r$, and taking into account that $\gamma_{r,0}^{(n)} = 0$, we may bound

$$\mathbb{V}(C_{m,r}^{(n)}) \leq \omega_{r,r}^{(n)} \left[ \binom{m}{r}^2 - \binom{m}{r} \binom{m-r}{r} \right] \leq \omega_{r,r}^{(n)} \left[ \binom{m}{r} \binom{m-r}{r} \right] \leq C_r \omega_{r,r}^{(n)} m^2r^{-1}.$$

Since $\mathbb{E}(c_{m,r}^{(n)}) = \binom{m}{r}\mu_{r-1}^{(n)}$, the second condition of Lemma 7.2 is satisfied, with $\delta = 2 - \frac{1}{r}$. □

For $2c_{m,r}^{(n)}$ and even further for its $q$ moment version, there are analogous strong laws.
For completeness, a proof of Lemma 7.2 (modeled upon [13], Theorem 6.8) follows.

**Proof of Lemma 7.2.** Chebyshev’s inequality gives

\[
\Pr \left( \left| \frac{Y_m}{E(Y_m)} - 1 \right| > \lambda \right) \leq \frac{1}{\lambda^2} \frac{\text{Var}(Y_m)}{E(Y_m)^2} \leq \frac{1}{\lambda^2} \frac{1}{E(Y_m)^{2-\delta}}.
\]

This ensures that the subsequence

\[
\frac{Y_{m_k}}{E(Y_{m_k})} \xrightarrow{a.s.} 1 \text{ as } k \to \infty,
\]

if \( m_k = \lfloor k^{(2-\delta)/\beta} \rfloor \). Now, for each \( m \), such \( m_k \leq m < m_{k+1} \),

\[
\frac{Y_m}{E(Y_m)} \leq \frac{Y_{m_{k+1}}}{E(Y_{m_{k+1}})} \frac{E(Y_{m_{k+1}})}{E(Y_{m_k})}.
\]

Since \( m_{k+1}/m_k \to 1 \) as \( k \to \infty \), and because of the polynomial rate condition, we deduce that, almost surely,

\[
\limsup_{m \to \infty} \frac{Y_m}{E(Y_m)} \leq 1
\]

An analogous estimate from below completes the proof. \( \square \)

**References**

[1] Baldi, P. and Rinott, Y.: Asymptotic normality of some graph related statistics. *J. Appl. Prob.* 26, (1989), 171–175.

[2] Baldi, P. and Rinott, Y.: On normal approximations of distributions in terms of dependency graphs. *Ann. Probab.* 17 (1989), no. 4, 1646–1650.

[3] Brown, T., C. and Silverman, B. W.: Rates of Poisson convergence for U-statistics. *J. Appl. Prob.* 16 (1979), 428–432.

[4] Cai, J.-Y. and Bach, E.: On testing for zero polynomials by a set of points with bounded precision. In *COCOON 2001*, 473–482. Lect. Notes Comput Sci. 2108, Springer Verlag, 2001.

[5] Cesàro, E.: Étude moyenne du plus grand commun diviseur de deux nombres. *Annali di Matematica Pura ed Applicata* (Tortolini, etc.). Rome. 13 (1885), 235–250.

[6] Cesàro, E.: Sur le plus grand commun diviseur de plusieurs nombres. *Annali di Matematica Pura ed Applicata* 13 (1885), 291–294.

[7] Christopher, J.: The asymptotic density of ome k-dimensional sets. *Amer. Math. Monthly* 63 (1956), no. 6, 399–401.

[8] Cohen, E.: Arithmetical functions of a greatest common divisor. I. *Proc. Amer. Math. Soc.* 11 (1960), no. 2, 164–171.

[9] Darling, R. W. R. and Pyle, E. E.: Maximum gcd among pairs of random integers. *Integers* 11 (2011), no. 2, 93–105.

[10] Delange, H.: Théorèmes taubériens et applications arithmétiques. *Séminaire Delange–Pisot–Poitou. Théorie des nombres*, tome 4 (1962-1963), exposé n° 16, pages 1–17. http://www.numdam.org.

[11] Diaconis, P.: Asymptotic expansions for the mean and the variance of the number of prime factors on a number n. Technical Report no. 96, Stanford University, 1976.

[12] Diaconis, P. and Erdős, P.: On the distribution of the greatest common divisor. Technical Report no. 12, Stanford University, 1977. Reprinted in *A Festschrift for Herman Rubin*, 56–61. Lecture Notes, Monograph Series, vol. 45, Institute of Mathematical Statistics, 2004.
[13] Durrett, R.: *Probability: Theory and examples*. Second edition. Wadsworth Publishing Company. 1966.

[14] Fernández, J. L., Fernández, P.: On the probability distribution of gcd and lcm of $r$-tuples of integers. Preprint, 2013. Arxiv: 1305.0536.

[15] Golomb, S. W.: A class of probability distributions on the integers. *J. Number Theory* 2 (1970), 189–192.

[16] Janson, S.: Normal convergence by higher semiinvariants with applications to sums of dependent random variables and random graphs. *Ann. Probab.* 16 (1988), no. 1, 305–312.

[17] Hardy, G. H. and Wright, E. M.: *An introduction to the Theory of Numbers*. Oxford Science Publications, Oxford, 1979.

[18] Herzog, F. and Stewart, B.: Patterns of visible and non visible lattices. *Amer. Math. Monthly* 78 (1971), 487–496.

[19] Hoeffding, W.: A class of statistics with asymptotically normal distributions. *Ann. Math. Statist.* 19 (1948) 293-325.

[20] Hu, J.: Pairwise relative primality of positive integers. Preprint, 2013.

[21] Hwang, H.-K.: Asymptotic behaviour of some infinite products involving prime numbers. *Acta Arith.* 75 (1996), 339-350. Corrigenda in *Acta Arith.* 87 (1999), 391.

[22] Kac, M.: *Statistical independence in Probability, Analysis and Number Theory*. Carus mathematical Monographs, Mathematical Association of America, 1959.

[23] Kingman, J. F. C.: The Poisson–Dirichlet distribution and the frequency of large prime divisors, 2004. http://www.newton.cam.ac.uk/preprints/NI04019.pdf.

[24] Lehmer, D. H.: A conjecture of Krishnaswami. *Bull. Amer. Math. Soc.* 54 (1948), no. 12, 1185–1190.

[25] Lehmer, D. N.: Asymptotic evaluation of certain totient-sums. *Amer. J. Math.* 22 (1900), no. 4, 293–335.

[26] Lloyd, S. P.: Ordered prime divisors of a random integer. *Ann. Prob.* 12 (1984), no. 4, 1205–1212.

[27] Nymann, J. E.: On the probability that $k$ positive integers are relatively prime. *J. Number Th.* 4 (1972) 469-473.

[28] Serfling, R.: *Approximation theorems of Mathematical Statistics*. Wiley Series in Probability and Mathematical Statistics, John Wiley, 1980.

[29] Silverman, B. and Brown, T.: Short distances, flat triangles and Poisson limits. *J. Appl. Prob.* 15 (1978), no. 4, 815–823.

[30] Toth, L.: The probability that $k$ positive integers are pairwise relatively prime. *Fibonacci Quart.* 40 (2002), 13–18.

[31] Toth, L.: A survey of gcd-sum functions. *J. Integer Seq.* 13 (2010), 1–23.

José L. Fernández: Departamento de Matemáticas, Universidad Autónoma de Madrid, 28049-Madrid, Spain. joseluis.fernandez@uam.es

Pablo Fernández: Departamento de Matemáticas, Universidad Autónoma de Madrid, 28049-Madrid, Spain. pablo.fernandez@uam.es

The research of both authors is partially supported by Fundación Akusmatika. The second named author is partially supported by the Spanish Ministerio de Ciencia e Innovación, project no. MTM2011-22851.

32