LIMITING JOINT DISTRIBUTION OF GREATEST COMMON DIVISORS IN RANDOM HYPERCUBES

ISTVÁN KOLOSSVÁRY

Abstract. The limiting distribution of the greatest common divisor (gcd) of a D-tuple of random natural numbers is known. We generalise this by determining an infinite product representation for the joint distribution of gcd-s in a D-dimensional hypercube of fixed but arbitrary side length around a D-tuple of random natural numbers. This allows for calculation of any statistic of the gcd-s within this hypercube, such as the number of coprime D-tuples.

1. Introduction and main results

Using the unique prime factorisation of each natural number $N = \prod_{p\in\mathcal{P}} p^{\nu_p(N)}$, where $\mathcal{P}$ denotes the set of primes and $\nu_p(N)$ is the p-adic valuation of N, the *greatest common divisor* (gcd) of a D-tuple of strictly positive integers $N_1,\dots,N_D$ is

$$\gcd(N_1,\dots,N_D) := \prod_{p\in\mathcal{P}} p^{\min_{1\le j\le D}\nu_p(N_j)}.$$

For brevity, we denote a D-tuple by $\mathbf{N}_D := (N_1,\dots,N_D)$ moreover, multiplication by a scalar $c\cdot\mathbf{N}_D = (c\cdot N_1,\dots,c\cdot N_D)$ and addition $\mathbf{N}_D+\mathbf{j} = (N_1+j_1,\dots,N_D+j_D)$ are done coordinate-wise. It is well-known that the limiting density of coprime pairs, i.e. when $\gcd(N_1,N_2)=1$, usually attributed to Dirichlet [3], is

$$\lim_{n\to\infty}\frac{1}{n^2}\#\big\{(N_1,N_2)\in\{1,\dots,n\}^2 : \gcd(N_1,N_2)=1\big\} = \frac{6}{\pi^2} = \frac{1}{\zeta(2)}. \tag{1.1}$$

Recall the Riemann zeta function $\zeta(s)$ and Euler's product formula

$$\zeta(s) := \sum_{k=1}^{\infty}\frac{1}{k^s} = \prod_{p\in\mathcal{P}}(1-p^{-s})^{-1}$$

for $\Re(s)>1$. The limit in (1.1) has since initiated an abundance of research. Most notably for the purpose of this paper, the limiting distribution of $\gcd(\mathbf{N}_D)$ taking any value a is

$$\lim_{n\to\infty}\frac{1}{n^D}\#\big\{\mathbf{N}_D\in\{1,\dots,n\}^D : \gcd(\mathbf{N}_D)=a\big\} = \frac{1}{a^D\cdot\zeta(D)}. \tag{1.2}$$

This already appears in the work of Cesàro [1] and also follows from the more general setting of Chidambaraswamy and Sitaramachandrarao [2], who also gave bounds on the error. For a comprehensive list of references in the area, see the survey [4].

One natural direction for generalisation is to consider the joint distribution of gcd-s in a 'window' around the point $\mathbf{N}_D$. Very recently, for $D=2$, Fernández and Fernández [5] consider an $M\times M$ square $(N_1+j_1,N_2+j_2)_{j_1,j_2=1}^{M}$ as the 'window'and determine the limiting distribution of the function counting the number of coprime pairs in a random $M\times M$ square. Knowledge of the joint distribution of gcd-s would already imply the distribution of coprime pairs. The main objective of the current paper is to determine the limiting joint distribution of gcd-s in random M^D-hypercubes, thus generalising all aforementioned results.

2020 *Mathematics Subject Classification.* Primary 11A05 11N25 Secondary 11K65 11B75

Key words and phrases. greatest common divisor, random samples of integers, limiting distribution, coprime tuples.

Formally, let M be a strictly positive integer and $\mathbf{N}_D$ be a D-tuple of strictly positive integers. We consider the 'window' $\mathcal{W}_M^D := \{0,1,\dots,M-1\}^D$ around $\mathbf{N}_D$ and the M^D-array of gcd-s

$$\mathrm{GCD}_M(\mathbf{N}_D) := \big(\gcd(\mathbf{N}_D+\mathbf{j})\big)_{\mathbf{j}\in\mathcal{W}_M^D}$$

derived from it. Let

$$\mathcal{A}_M^D := \big\{A\in\mathbb{N}^{M^D} : (\exists \mathbf{N}_D\in\mathbb{N}^D),\ \mathrm{GCD}_M(\mathbf{N}_D)=A\big\}$$

denote the set of M^D-arrays which can be attained. Thus the goal of the paper is to characterise the set $\mathcal{A}_M^D$ and establish that the limit

$$\lim_{n\to\infty}\frac{1}{n^D}\#\big\{\mathbf{N}_D\in\{1,\dots,n\}^D : \mathrm{GCD}_M(\mathbf{N}_D)=A\big\} \tag{1.3}$$

exists, moreover, determine its value for all $A\in\mathcal{A}_M^D$.

Throughout, we adopt a probabilistic formulation of the problem. Let $\mathbf{N}_D^{(n)}=(N_1^{(n)},\dots,N_D^{(n)})$ denote a D-tuple of independent random variables all chosen uniformly from the set $\mathbb{N}_n := \{1,\dots,n\}$. Furthermore, let $\mathbf{P}_n$ denote the uniform distribution on $\mathbb{N}_n^D$, i.e. $\mathbf{P}_n(E)=\#E/n^D$ for any $E\subseteq\mathbb{N}_n^D$. With this notation, the limit (1.3) can be rewritten as

$$\lim_{n\to\infty}\mathbf{P}_n\big(\mathrm{GCD}_M(\mathbf{N}_D^{(n)})=A\big).$$

1.1. **Main results.** Before stating the main results, we introduce some notation. For any $m\in\mathbb{N}$, let $\mathcal{P}_m := \{p\in\mathcal{P} : p\le m\}$. Occasionally, we index an M^D-array $A=(a_{\mathbf{j}})_{\mathbf{j}\in\mathcal{W}_M^D}\in\mathbb{N}^{M^D}$ simply with $a\in A$. Let

$$\mathcal{P}(A) := \big\{p\in\mathcal{P} : (\exists a\in A),\ p\mid a\big\}$$

denote the set of all primes which divide some element of A. For each $p\in\mathcal{P}(A)$ define

$$T_A(p) := \max\{t\in\mathbb{N} : (\exists a\in A),\ p^t\mid a\}.$$

It can be considered as the 'p-adic valuation of A'. Also introduce the set of indices

$$\mathcal{J}_A(p) := \big\{\mathbf{j}\in\mathcal{W}_M^D : p^{T_A(P)}\mid a_{\mathbf{j}}\big\}.$$

A trivial observation is that if $A\in\mathcal{A}_M^D$, then

$$\#\big(\mathcal{J}_A(p)\cap\{0,1,\dots,\min\{p^{T_A(p)}-1,M-1\}\}^D\big)=1 \tag{1.4}$$

for each $p\in\mathcal{P}(A)$ simply because in each coordinate of a gcd array we take consecutive numbers and $p^{T_A(p)}$ divides exactly one of $\min\{p^{T_A(p)},M\}$ consecutive numbers. Throughout, if (1.4) holds, then this unique index is denoted by $\mathbf{j}_A(p)$. It is the 'origin' of the grid

$$\mathcal{G}_A(p) := \{\mathbf{j}_A(p)+p^{T_A(p)}\cdot\mathbb{Z}^D\}\cap\mathcal{W}_M^D.$$

Note that if $\mathbf{j}_A(p)+p^{T_A(p)}\cdot\mathbf{z}\in\mathcal{G}_A(p)$, then in fact all coordinates of $\mathbf{z}$ are from the set $\{0,1,\dots,p-1\}$. More precisely, there must exist a coordinate $1\le d_A(p)\le D$ such that

$$(\mathbf{j}_A(p))_{d_A(p)}+(p-1)p^{T_A(p)}\ge M, \tag{1.5}$$

otherwise, $T_A(p)$ would not be maximal. This implies that $\#\mathcal{G}_A(p)\le(p-1)\cdot p^{D-1}<p^D$. The sets $\mathcal{P}(A)$ and $\{(T_A(p),\mathbf{j}_A(p),\mathcal{G}_A(p)) : p\in\mathcal{P}(A)\}$ are deterministic functions of $A\in\mathcal{A}_M^D$. Some immediate observations are that $M<\min_{p\in\mathcal{P}(A)}p^{T_A(p)+1}$ since $T_A(p)$ is maximal, furthermore, if $M\le p^{T_A(p)}$ then $\mathcal{G}_A(p)=\{\mathbf{j}_A(p)\}$.

Any $A\in\mathcal{A}_M^D$ has a very particular structure with respect to how each $p\in\mathcal{P}(A)$ divides the elements of A. For each $\mathbf{k}\in\mathcal{W}_M^D$ we define

$$R_{A,p}(\mathbf{k}) := \max\{r\in\{0,1,\dots\} : (\exists\mathbf{z}\in\mathbb{Z}^D),\ \mathbf{k}=\mathbf{j}_A(p)+p^r\cdot\mathbf{z}\}.$$

Observe that if $A\in\mathcal{A}_M^D$, then $R_{A,p}(\mathbf{k})\le T_A(p)$ with equality if and only if $\mathbf{k}\in\mathcal{G}_A(p)$, in fact $\mathcal{J}_A(p)=\mathcal{G}_A(p)$. We say that $p\in\mathcal{P}(A)$ *divides A properly* if

$$\text{(1.4) and (1.5) hold, moreover, } \nu_p(a_{\mathbf{k}})=R_{A,p}(\mathbf{k}) \text{ for every } \mathbf{k}\in\mathcal{W}_M^D.$$

See Figure 1 for an illustration of the introduced notions and also § 3.1 for some concrete examples of gcd arrays. We are now ready to state our main results.

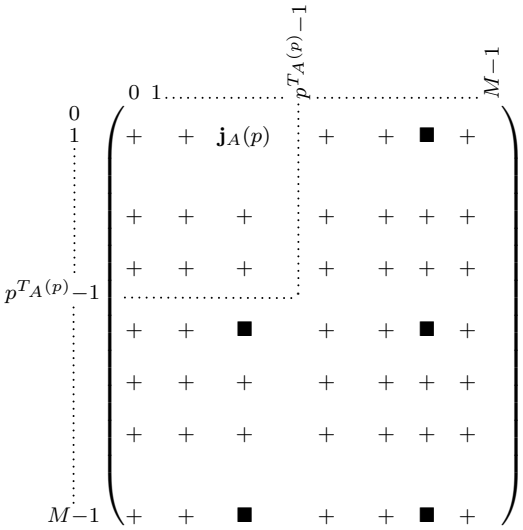

FIGURE 1. An illustration of the notion that p divides A properly. Here we chose $D = 2$, $M = 20$, $p = 3$, $T_A(p) = 2$ and $\mathbf{j}_A(p) = (1, 6)$. Indices labeled by ■ and $\mathbf{j}_A(p)$ are the elements of $\mathcal{G}_A(p)$, the corresponding elements of A have 3-adic valuation equal to 2, while the ones marked with + have 3-adic valuation equal to 1 and the rest are not divisible by 3.

Proposition 1.1. *An M^D-array A is an element of $\mathcal{A}_M^D$ if and only if $\mathcal{P}_M \subseteq \mathcal{P}(A)$ and p divides A properly for every $p \in \mathcal{P}(A)$.*

Theorem 1.2. *Assume $A \in \mathcal{A}_M^D$. Then*

$$\lim_{n\to\infty} \mathbf{P}_n\big(\mathrm{GCD}_M(\mathbf{N}_D^{(n)}) = A\big) = \prod_{p\in\mathcal{P}(A)} \frac{1}{p^{T_A(p)\cdot D}} \left(1 - \frac{\#\mathcal{G}_A(p)}{p^D}\right) \prod_{p\notin\mathcal{P}(A)} \left(1 - \left(\frac{M}{p}\right)^D\right) > 0.$$

Remark 1.3. *Any attainable M^D-array has strictly positive density. The formula for $M = 1$ readily simplifies to $(a^D \cdot \zeta(D))^{-1}$ in (1.2). The formula also naturally encodes conditions (1.5) and $\mathcal{P}_M \subseteq \mathcal{P}(A)$. Indeed, if (1.5) does not hold for some p, then $\#\mathcal{G}_A(p) \geq p^D$ resulting in $1 - \#\mathcal{G}_A(p)/p^D \leq 0$. Similarly, if $\mathcal{P}_M \setminus \mathcal{P}(A) \neq \emptyset$, then $1 - (M/p)^D \leq 0$ for any $p \in \mathcal{P}_M \setminus \mathcal{P}(A)$.*

The proofs are in § 2. The proof of Theorem 1.2 builds on arguments of a previous work of the author [6]. The advantage of the argument is that it is short and completely elementary, but it does not give estimates on the rate of convergence. A natural line of further study would be to give bounds on the error. Other directions to pursue could be to consider more general 'windows'. The "shape" of the 'window' need not be a hypercube or instead of evaluating the gcd of consecutive numbers one could rather take the value of non-constant polynomials with integer coefficients like in [2]. Instead of taking the limit of the uniform distribution, one could also consider different probabilities, see [4, § 1.3.]. Section 3 contains some further discussion.

1.2. **Applications.** Theorem 1.2 naturally defines a random variable $Z_\infty = Z_\infty(M, D)$ on $\mathcal{A}_M^D$ with probability distribution given by

$$\mathbf{P}(Z_\infty = A) \coloneqq \prod_{p\in\mathcal{P}(A)} \frac{1}{p^{T_A(p)\cdot D}} \left(1 - \frac{\#\mathcal{G}_A(p)}{p^D}\right) \prod_{p\notin\mathcal{P}(A)} \left(1 - \left(\frac{M}{p}\right)^D\right).$$

A reformulation of Theorem 1.2 is that the random variable $\mathrm{GCD}_M(\mathbf{N}_D^{(n)})$ tends in distribution to Z_∞ as $n \to \infty$. With knowledge of the precise distribution of Z_∞, at least in principle it is possible to determine the probability of any subset $\mathcal{E} \subseteq \mathcal{A}_M^D$ simply by evaluating the sum $\sum_{A\in\mathcal{E}} \mathbf{P}(Z_\infty = A)$. In particular,

$$Z_M^D(A) \coloneqq \#\{a \in A : a = 1\}$$

counts the number of 1 entries in the array A, hence, $Z_M^D\big(\mathrm{GCD}_M(\mathbf{N}_D)\big)$ counts the number of (fully) coprime D-tuples in the window starting at $\mathbf{N}_D$. Theorem 1.2 immediately implies the following.

Corollary 1.4. *For any $r \in \{0, 1, \dots, M^D\}$,*

$$\lim_{n\to\infty} \mathbf{P}_n\big(Z_M^D\big(\mathrm{GCD}_M(\mathbf{N}_D^{(n)})\big) = r\big) = \sum_{\substack{A\in\mathcal{A}_M^D \\ Z_M^D(A)=r}} \mathbf{P}(Z_\infty = A).$$

Therefore, our work also generalises [5], since it corresponds to the special case $D = 2$. Their proof is also probabilistic in nature, though very distinct from ours. In fact, their formula is a finite sum, which makes it more convenient for calculations, see § 3 for further discussion.

Equally straightforward, at least in principle, is to determine the expectation of some real valued function of Z_∞. For example, let

$$\widehat{A^t} \coloneqq \frac{1}{M^D}\sum_{a\in A} a^t$$

be the average of the sum of the t-th powers of the elements of $A \in \mathcal{A}_M^D$ for some $t \geq 1$.

Corollary 1.5. *Assume $f : \mathcal{A}_M^D \to \mathbb{R}$. Then*

$$\mathbf{E}f(Z_\infty) = \sum_{A\in\mathcal{A}_M^D} f(A)\cdot\mathbf{P}(Z_\infty = A).$$

In particular, $\mathbf{E}\,\widehat{Z_\infty^t} = \infty$ if and only if $t \geq D - 1$ irrespective of M.

Proof. The formula for $\mathbf{E}f(Z_\infty)$ is just the definition of expectation. Assume $1 \leq t < D - 1$. Using that $\max_{a\in A} a \leq \prod_{p\in\mathcal{P}(A)} p^{T_A(p)}$ and $1 \leq \min\{\mathcal{G}_A(p), M\}$, we can bound

$$\begin{aligned}\mathbf{E}\,\widehat{Z_\infty^t} &\leq \sum_{A\in\mathcal{A}_M^D}\prod_{p\in\mathcal{P}(A)} p^{T_A(p)(t-D)}\prod_{p\in\mathcal{P}}\left(1-\frac{1}{p^D}\right)\\ &= \frac{1}{\zeta(D)}\sum_{k=2}^{\infty}\#\Big\{A\in\mathcal{A}_M^D : \prod_{p\in\mathcal{P}(A)} p^{T_A(p)} = k\Big\}\cdot k^{t-D}.\end{aligned}$$

Recall that the prime omega function $\omega(k) \leq \log\log k + B_1 + O((\log k)^{-1})$ for almost all integers k, where B_1 is the Mertens constant. This together with the observation that the pairs $\{(\mathbf{j}_A(p), T_A(p)) : p \in \mathcal{P}(A)\}$ determine A gives the bound

$$\#\Big\{A\in\mathcal{A}_M^D : \prod_{p\in\mathcal{P}(A)} p^{T_A(p)} = k\Big\} \leq O\big(M^{D\log\log k}\big) = O\big((\log k)^{D\log M}\big)$$

for almost all integers k. Finiteness of $\mathbf{E}\,\widehat{Z_\infty^t}$ now follows by the choice of t.

Now assume $t \geq D - 1$. Since $1 \leq \#\mathcal{G}_A(p) \leq (p-1)\cdot p^{D-1}$, $\#\mathcal{G}_A(p) = 1$ for all $p \geq M$ and $D \geq 2$, there exists $C_0 = C_0(M, D) > 0$ such that

$$\prod_{p\in\mathcal{P}(A)}\left(1-\frac{\#\mathcal{G}_A(p)}{p^D}\right)\prod_{p\notin\mathcal{P}(A)}\left(1-\Big(\frac{M}{p}\Big)^D\right) \geq \Big(\prod_{p\leq M}\frac{1}{p}\Big)\cdot\prod_{p>M}\left(1-\Big(\frac{M}{p}\Big)^D\right) \geq C_0.$$

For each $m > M$, we define $B^{(m)} = (b^{(m)}_{\mathbf{j}})_{\mathbf{j}\in\mathcal{W}^D_M}$ as follows. Let $b^{(m)}_{\mathbf{0}} := m \cdot \prod_{p\in\mathcal{P}_M\setminus\mathcal{P}(m)} p$ and continue 'filling out' $B^{(m)}$ so that each $p \in \mathcal{P}_M \cup \mathcal{P}(m)$ divides $B^{(m)}$ properly. By Proposition 1.1 we have that $B^{(m)} \in \mathcal{A}^D_M$. We use that $\sum_{b\in B^{(m)}} b^t \geq m^{D-1}$; $T_A(p) = 1$ for each $p \geq M$ and $T_A(p) \leq \log_2 M$ for every $p < M$ in order to bound

$$\mathbf{E}\,\widehat{Z^t_\infty} \geq \sum_{m=1}^{\infty} \frac{\sum_{b\in B^{(m)}} b^t}{M^D} \cdot \mathbf{P}(Z_\infty = B^{(m)}) \geq \frac{C_0}{M^D} \sum_{m=1}^{\infty} \frac{m^{D-1}}{m^D \prod_{p\in\mathcal{P}_M} p^{D\cdot\log_2 M}} = \infty.$$

□

2. Proofs

We prove Proposition 1.1 and Theorem 1.2 in separate subsections. In this section we use $\mathbf{N}_D \pmod p = \mathbf{j}$ to abbreviate '$N_k \pmod p = j_k$ for every $1 \leq k \leq D$' or $\mathbf{N}_D \pmod p \in E_1 \times \ldots \times E_D$ for '$N_k \pmod p \in E_k$ for every $1 \leq k \leq D$'.

2.1. **Proof of Proposition 1.1.** Fix $A \in \mathcal{A}^D_M$, i.e. there exists a D-tuple $\mathbf{N}_D$ such that $\mathrm{GCD}_M(\mathbf{N}_D) = A$. Trivially $\mathcal{P}_M \subseteq \mathcal{P}(A)$ since for every $p \in \mathcal{P}_M$ there must exist an index $\mathbf{k}(p) \in \mathcal{W}^D_M$ such that $p \mid a_{\mathbf{k}(p)}$. Fix arbitrary $p \in \mathcal{P}(A)$. Condition (1.4) trivially holds. It is also clear that (1.5) is a necessary condition, otherwise, there would exist an index $\mathbf{k} \in \mathcal{W}^D_M$ such that $\nu_p(\gcd(\mathbf{N}_D + \mathbf{k})) > T_A(p)$ which contradicts the maximality of $T_A(p)$. It remains to show that $\nu_p(a_{\mathbf{k}}) = R_{A,p}(\mathbf{k})$ for every $\mathbf{k} \in \mathcal{W}^D_M$. The prime p defines the triplet $(T_A(p), \mathbf{j}_A(p), \mathcal{G}_A(p))$, in particular, by definition $\nu_p(a_{\mathbf{j}_A(p)}) = T_A(p)$. The index $\mathbf{j}_A(p)$ can be thought of as the 'origin' of grids $\mathcal{G}^t_A(p) := \{\mathbf{j}_A(p) + p^t \cdot \mathbb{Z}^D\} \cap \mathcal{W}^D_M$ for all $t \leq T_A(p)$ in the sense that $p^t \mid \mathbf{N}_D + \mathbf{k}$ for all $\mathbf{k} \in \mathcal{G}^t_A(p)$ and as a result $p^t \mid a_{\mathbf{k}}$. For each $\mathbf{k} \in \mathcal{W}^D_M$, we defined $R_{A,p}(\mathbf{k})$ to be precisely the largest exponent t such that $\mathbf{k} \in \mathcal{G}^t_A(p)$. Therefore, $\nu_p(a_{\mathbf{k}}) = R_{A,p}(\mathbf{k})$ for every $\mathbf{k} \in \mathcal{W}^D_M$.

In the other direction, if $A \in \mathbb{N}^{M^D}$ is such that $\mathcal{P}_M \subseteq \mathcal{P}(A)$ and every $p \in \mathcal{P}(A)$ divides A properly, then we construct a D-tuple $\mathbf{N}_D$ using the Chinese remainder theorem such that $\mathrm{GCD}_M(\mathbf{N}_D) = A$. For each $p \in \mathcal{P}(A)$, the index $\mathbf{j}_A(p)$ is defined by (1.4) while the coordinate $d_A(p)$ is defined by (1.5). We set up the system of congruences by considering

$$\begin{cases} x_{d_A(p)} + \big(\mathbf{j}_A(p)\big)_{d_A(p)} & \equiv p^{T_A(p)} \pmod{p^{T_A(p)+1}}; \\ x_d + \big(\mathbf{j}_A(p)\big)_d & \equiv 0 \pmod{p^{T_A(p)}} \quad \text{for every } d \neq d_A(p). \end{cases}$$

This ensures that for each $\mathbf{k} \in \mathcal{G}_A(p)$ and any $\mathbf{x} = (x_1, \ldots, x_D)$ satisfying these congruences, we have that $\nu_p\big(\gcd(\mathbf{x}_D + \mathbf{k})\big) = T_A(p)$. (Taking simply $\mathbf{x} \equiv -\mathbf{j}_A(p) \pmod{p^{T_A(p)}}$ is not sufficient.) Considering these congruences simultaneously for all $p \in \mathcal{P}(A)$ gives a system of congruences for each element x_d of the D-tuple $\mathbf{x}$. We may now apply the Chinese remainder theorem to each x_d to obtain a D-tuple $\mathbf{N}_D$ with elements $1 \leq N_d \leq \prod_{p\in\mathcal{P}(A)} p^{T_A(p)+1}$. If $\mathcal{P}(\mathrm{GCD}_M(\mathbf{N}_D)) = \mathcal{P}(A)$, then by construction $\mathrm{GCD}_M(\mathbf{N}_D) = A$ and we are done. However, the construction may have resulted in an $\mathbf{N}_D$ such that $\mathcal{P}(\mathrm{GCD}_M(\mathbf{N}_D)) \supset \mathcal{P}(A)$. In such a case, for each $p \in \mathcal{P}(\mathrm{GCD}_M(\mathbf{N}_D)) \setminus \mathcal{P}(A)$, we can add the congruence $x_1 \equiv k_p \pmod p$ with $k_p \in \{1, 2, \ldots, p - M\}$ and get a new N'_1 with the Chinese remainder theorem. This ensures that $p \notin \mathcal{P}(\mathrm{GCD}_M(N'_1, N_2, \ldots, N_D))$. If $\mathcal{P}(\mathrm{GCD}_M(N'_1, N_2, \ldots, N_D)) = \mathcal{P}(A)$, then the procedure terminates, otherwise one can change the value of k_p or add new congruences and repeat. The procedure will terminate because the density of integers not divisible by any prime not in $\mathcal{P}(A)$ is at least $\prod_{p>M}(1 - (M/p)^D) > 0$. See § 3.1 for two concrete examples of arrays A for which we find an appropriate $\mathbf{N}_D$.

2.2. **Proof of Theorem 1.2.** The proof relies on the idea that 'divisibility by distinct primes are (asymptotically) independent events'. The Chinese remainder theorem implies that for distinct primes p and q the map

$$\begin{cases} \mathbb{Z}/pq\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ x \mapsto (x \pmod p, x \pmod q) \end{cases}$$

is a bijection. In particular, the random variables $x \mapsto x \,(\mathrm{mod}\, p)$ and $x \mapsto x \,(\mathrm{mod}\, q)$ are independent on $\mathbb{Z}/pq\mathbb{Z}$. Ultimately this is what leads to the infinite product representation of the formula in Theorem 1.2.

Proposition 2.1. *Fix $D \geq 1$ and a finite set $\mathcal{Q}$ of pairwise coprime integers. Let $\mathbf{N}_D^{(n)}$ be a uniformly chosen random variable on the set $\mathbb{N}_n^D$. Then as $n \to \infty$, the random array $\big(\mathbf{N}_D^{(n)} \,(\mathrm{mod}\, q)\big)_{q\in\mathcal{Q}}$ tends in distribution to an array of independent and uniform random variables on the space $\prod_{q\in\mathcal{Q}} \mathbb{Z}^D/q\mathbb{Z}^D$.*

Proof. For $D = 1$ this can be found in for example [7, Proposition 1.3.7.]. It naturally generalises to D-tuples since the elements of $\mathbf{N}_D^{(n)}$ are independent. □

A typical application of Proposition 2.1 is that if $\mathcal{Q} = \{q\}$ and $Z \subseteq \mathbb{Z}^D/q\mathbb{Z}^D$, then

$$\lim_{n\to\infty} \mathbf{P}_n\big(\mathbf{N}_D^{(n)} \,(\mathrm{mod}\, q) \in Z\big) = \frac{\#Z}{q^D}. \tag{2.1}$$

The next lemma explains why the different terms in the formula of Theorem 1.2 appear.

Lemma 2.2. *Let $\mathbf{N}_D^{(n)}$ be a uniformly chosen random variable on the set $\mathbb{N}_n^D$ and assume $A \in \mathcal{A}_M^D$. Then for $p \in \mathcal{P}$,*

$$\lim_{n\to\infty} \mathbf{P}_n\big(\mathbf{N}_D^{(n)} \,(\mathrm{mod}\, p) \in \{0, p-1, \dots, p-M+1\}^D\big) = \min\big\{M^D/p^D, 1\big\},$$

and for every $p \in \mathcal{P}(A)$,

$$\lim_{n\to\infty} \mathbf{P}_n\big((\forall \mathbf{k} \in \mathcal{G}_A(p)),\ \nu_p(\mathbf{N}_D^{(n)} + \mathbf{k}) = T_A(p)\big) = \frac{1}{p^{T_A(p)\cdot D}} - \frac{\#\mathcal{G}_A(p)}{p^{(T_A(p)+1)\cdot D}}.$$

Proof. The first claim is just a direct application of (2.1). It also shows why $\mathcal{P}_M \subseteq \mathcal{P}(A)$. As for the second claim, let us introduce the events

$$E_{A,p}^{(n)}(t, \mathbf{k}) := \{\mathbf{N}_D \in \mathbb{N}_n^D : p^t \mid \mathbf{N}_D + \mathbf{k}\} \quad \text{and} \quad \overline{E_{A,p}^{(n)}}(t, \mathbf{k}) := \{\mathbf{N}_D \in \mathbb{N}_n^D : p^t \nmid \mathbf{N}_D + \mathbf{k}\}.$$

With this notation, $\{\nu_p(\mathbf{N}_N^{(n)} + \mathbf{k}) = T_A(p)\} = E_{A,p}^{(n)}(T_A(p), \mathbf{k}) \cap \overline{E_{A,p}^{(n)}}(T_A(p)+1, \mathbf{k})$ for $\mathbf{k} \in \mathcal{G}_A(p)$. As a result,

$$\begin{aligned}
&\mathbf{P}_n\big((\forall \mathbf{k} \in \mathcal{G}_A(p)),\ \nu_p(\mathbf{N}_N^{(n)} + \mathbf{k}) = T_A(p)\big) \\
&\quad= \mathbf{P}_n\Big(\bigcap_{\mathbf{k}\in\mathcal{G}_A(p)} E_{A,p}^{(n)}(T_A(p), \mathbf{k}) \cap \overline{E_{A,p}^{(n)}}(T_A(p)+1, \mathbf{k})\Big) \\
&\quad= \mathbf{P}_n\Big(E_{A,p}^{(n)}(T_A(p), \mathbf{j}_A(p)) \cap \bigcap_{\mathbf{k}\in\mathcal{G}_A(p)} \overline{E_{A,p}^{(n)}}(T_A(p)+1, \mathbf{k})\Big) \\
&\quad= \mathbf{P}_n\big(E_{A,p}^{(n)}(T_A(p), \mathbf{j}_A(p))\big) - \mathbf{P}_n\Big(\bigcup_{\mathbf{k}\in\mathcal{G}_A(p)} E_{A,p}^{(n)}(T_A(p)+1, \mathbf{k})\Big) \\
&\quad= \mathbf{P}_n\big(E_{A,p}^{(n)}(T_A(p), \mathbf{j}_A(p))\big) - \sum_{\mathbf{k}\in\mathcal{G}_A(p)} \mathbf{P}_n\Big(E_{A,p}^{(n)}(T_A(p)+1, \mathbf{k})\Big) \\
&\quad\to \frac{1}{p^{T_A(p)\cdot D}} - \frac{\#\mathcal{G}_A(p)}{p^{(T_A(p)+1)\cdot D}}
\end{aligned}$$

as $n \to \infty$ by another simple application of (2.1). The second equality follows from the grid structure of $\mathcal{G}_A(p)$; the third one from De Morgan's law; and the fourth one holds because of inclusion-exclusion since for any given $\mathbf{N}_D$ there can be at most one $\mathbf{k} \in \mathcal{G}_A(p)$ for which $p^{T_A(p)+1} \mid \mathbf{N}_D + \mathbf{k}$, i.e. the events $E_{A,p}(T_A(p)+1, \mathbf{k})$ are mutually exclusive for $\mathbf{k} \in \mathcal{G}_A(p)$. □

Proof of Theorem 1.2. Let $A \in \mathcal{A}_M^D$ be fixed and introduce $\mathcal{N}_A := \{\mathbf{N}_D \in \mathbb{N}^D : \mathrm{GCD}_M(\mathbf{N}_D) = A\} \neq \emptyset$. The goal is to determine the divisibility restrictions that A imposes on $\mathbf{N}_D \in \mathcal{N}_A$. Recall that A uniquely determines the sets $\mathcal{P}(A)$ and $\{(T_A(p), \mathbf{j}_A(p), \mathcal{G}_A(p)) : p \in \mathcal{P}(A)\}$.

Let us begin with primes $p \notin \mathcal{P}(A)$. Observe that $p > M$ for all $p \notin \mathcal{P}(A)$. If $\mathbf{N}_D \in \mathcal{N}_A$, then

$$p \in \mathcal{P}(A) \iff \mathbf{N}_D \,(\mathrm{mod}\, p) \in \{0, p-1, \dots, p-M+1\}^D. \tag{2.2}$$

More interesting is when $p \in \mathcal{P}(A)$. If $\mathbf{N}_D \in \mathcal{N}_A$, then for every $\mathbf{k} \in \mathcal{W}_M^D$,

$$a_{\mathbf{k}} = \gcd(\mathbf{N}_D + \mathbf{k}) = \prod_{p \in \mathcal{P}(A)} p^{R_{A,p}(\mathbf{k})}.$$

Furthermore, as discussed already in § 2.1, since p divides A properly, the condition $\nu_p(\mathbf{N}_D + \mathbf{j}_A(p)) = T_A(p)$ already implies that $\nu_p(\mathbf{N}_D + \mathbf{k}) = R_{A,p}(\mathbf{k})$ for all $\mathbf{k} \in \mathcal{W}_M^D \setminus \mathcal{G}_A(p)$, but $\nu_p(\mathbf{N}_D + \mathbf{k}) = T_A(p)$ is not guaranteed for $\mathbf{k} \in \mathcal{G}_A(p)$. Therefore, $\mathbf{N}_D \in \mathcal{N}_A$ must satisfy that

$$(\forall p \in \mathcal{P}(A))\,(\forall \mathbf{k} \in \mathcal{G}_A(p)),\ \nu_p(\mathbf{N}_D + \mathbf{k}) = T_A(p). \tag{2.3}$$

Combining (2.2) and (2.3), we obtain for $n > \max_{p \in \mathcal{P}(A)} p^{T_A(p)}$ that the event

$$\begin{aligned}\big\{\mathrm{GCD}_M(\mathbf{N}_D^{(n)}) = A\big\} = \big\{&(\forall p \in \mathcal{P}(A))\,(\forall \mathbf{k} \in \mathcal{G}_A(p)),\ \nu_p(\mathbf{N}_D^{(n)} + \mathbf{k}) = T_A(p)\big\} \\ &\cap \big\{(\forall p \notin \mathcal{P}(A)),\ \mathbf{N}_D^{(n)} \,(\mathrm{mod}\, p) \in \{0, 1, \dots, p-1\}^D \setminus \{0, p-1, \dots, p-M+1\}^D\big\}.\end{aligned}$$

Notice that it is enough to take $p \in \mathcal{P}_{n+M-1} \setminus \mathcal{P}(A)$ in the second part because the condition automatically holds for all $p > n + M - 1$.

For $n \geq L > \max_{p \in \mathcal{P}(A)} p^{T_A(p)}$, let us introduce the event

$$\begin{aligned}E_L(n) := \big\{&(\forall p \in \mathcal{P}(A))\,(\forall \mathbf{k} \in \mathcal{G}_A(p)),\ \nu_p(\mathbf{N}_D^{(n)} + \mathbf{k}) = T_A(p)\big\} \cap \\ &\big\{(\forall p \in \mathcal{P}_{L+M-1} \setminus \mathcal{P}(A)),\ \mathbf{N}_D^{(n)} \,(\mathrm{mod}\, p) \in \{0, 1, \dots, p-1\}^D \setminus \{0, p-1, \dots, p-M+1\}^D\big\}.\end{aligned}$$

Then $E_n(n) = \big\{\mathrm{GCD}_M(\mathbf{N}_D^{(n)}) = A\big\}$. We claim that

$$\lim_{n\to\infty} \mathbf{P}_n\big(\mathrm{GCD}_M(\mathbf{N}_D^{(n)}) = A\big) = \lim_{L\to\infty} \lim_{n\to\infty} \mathbf{P}_n(E_L(n)).$$

Fix a large L and observe that the sequence $(E_L(n))_{n \geq L}$ as subsets of $\mathbb{N}^D$ is non-decreasing, i.e $E_L(n) \subseteq E_L(n+1)$. Hence, the set-theoretic limit $E_L := \lim_{n\to\infty} E_L(n)$ exists. Since $\mathcal{P}(A) \cup \mathcal{P}_{L+M-1} \setminus \mathcal{P}(A)$ is a finite set, we can apply Proposition 2.1 and Lemma 2.2 to calculate the limit

$$\lim_{n\to\infty} \mathbf{P}_n(E_L(n)) = \prod_{p \in \mathcal{P}(A)} \frac{1}{p^{T_A(p)\cdot D}} \left(1 - \frac{\#\mathcal{G}_A(p)}{p^D}\right) \prod_{p \in \mathcal{P}_{L+M-1} \setminus \mathcal{P}(A)} \left(1 - \left(\frac{M}{p}\right)^D\right).$$

Letting $L \to \infty$ gives precisely the formula in Theorem 1.2. For any n and $L < n$, we have $E_L(n) \supseteq E_{L+1}(n)$, which non-increasing property is passed onto the limit sequence $(E_L)_L$. As a result, the set-theoretic limit $E := \lim_{L\to\infty} E_L$ exists. Furthermore, $E_n(n) \subseteq E_{n+1}(n+1)$, so the limit $\lim_{n\to\infty} E_n(n)$ also exists and in fact is equal to E which concludes the proof. □

Remark 2.3. *The same strategy could be used to prove the following simpler statement. For any finite subset $\mathcal{P}_M \subseteq \mathcal{Q} \subset \mathcal{P}$ the limit*

$$\lim_{n\to\infty} \mathbf{P}_n(\mathcal{P}(\mathrm{GCD}_M(\mathbf{N}_D^{(n)})) = \mathcal{Q}) = \prod_{p \in \mathcal{Q}} \min\{(M/p)^D, 1\} \prod_{p \notin \mathcal{Q}} \left(1 - \left(\frac{M}{p}\right)^D\right) > 0.$$

3. Further discussion

In this section we give additional context to our results by giving (non-)examples of gcd arrays and looking more closely when the side-length of the 'window' is 2 or 3.

3.1. **Examples and non-examples of gcd arrays.** The following examples are clearly not gcd arrays:

$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 2 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 6 & 1 & 2 \\ 1 & 1 & 1 \\ 2 & 1 & 2 \end{bmatrix}.$$

The first one because $2 \notin \mathcal{P}(A)$. The second one does not satisfy (1.4), so 2 does not divide A properly. In the last one, 3 divides A properly, but 2 does not because (1.5) does not hold (one of the four corners must be divisible by 4).

In contrast, the following 7×7 array

$$A = \begin{bmatrix} 210 & 1 & 2 & 3 & 2 & 5 & 6 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 1 & 4 & 1 & 2 & 1 & 4 \\ 3 & 1 & 1 & 3 & 1 & 1 & 3 \\ 2 & 1 & 2 & 1 & 2 & 1 & 2 \\ 5 & 1 & 1 & 1 & 1 & 5 & 1 \\ 6 & 1 & 4 & 3 & 2 & 1 & 72 \end{bmatrix}$$

is an element of $\mathcal{A}_7^2$ due to Proposition 1.1 because $\mathcal{P}(A) = \mathcal{P}_7$, moreover, all of $2, 3, 5, 7$ divide A properly. For $p \in \mathcal{P}(A)$ the triplet $(T_A(p), \mathbf{j}_A(p), \mathcal{G}_A(p))$ is

p	2	3	5	7
$T_A(p)$	3	2	1	1
$\mathbf{j}_A(p)$	(6,6)	(6,6)	(0,0)	(0,0)
$\mathcal{G}_A(p)$	$\{(6,6)\}$	$\{(6,6)\}$	$\{(0,0),(0,5),(5,0),(5,5)\}$	$\{(0,0)\}$

Theorem 1.2 implies that

$$\lim_{n\to\infty} \mathbf{P}_n\big(\mathrm{GCD}_7(\mathbf{N}_2^{(n)}) = A\big) = \frac{1 - 4/5^2}{(2^3 \cdot 3^2 \cdot 5 \cdot 7)^2} \prod_{p\in\{2,3,7\}} \left(1 - \frac{1}{p^2}\right) \prod_{p>7} \left(1 - \frac{7^2}{p^2}\right) \approx 1.564 \times 10^{-8}.$$

The procedure in § 2.1 readily gives the example $\mathrm{GCD}_7((210, 2730)) = A$.

Another 4×4 example is

$$A = \begin{bmatrix} 3 & 2^5 & 1 & 2 \cdot 3^3 \\ 11^2 & 1 & 1 & 1 \\ 1 & 2 & 71 & 2 \\ 3 & 1 & 1 & 3 \end{bmatrix}.$$

One can check that $A \in \mathcal{A}_4^2$ with $\mathcal{P}(A) = \{2, 3, 11, 71\}$. Moreover, $\mathbf{P}(Z_\infty = A) \approx 2.02 \times 10^{-15}$ and $\mathrm{GCD}_4((637\,791, 787\,104)) = A$.

3.2. **Special case when $M = 2$.** The formula in Theorem 1.2 simplifies if we take the side-length of the 'window' to be 2. If $A \in \mathcal{A}_2^D$, then for every $p \in \mathcal{P}(A)$ there exists a unique index $\mathbf{k} \in \mathcal{W}_2^D$ such that $p \mid a_{\mathbf{k}}$, in fact $\mathbf{k} = \mathbf{j}_A(p)$. Therefore, $\#\mathcal{G}_A(p) = 1$ for every $p \in \mathcal{P}(A)$, and as a result, we obtain that

$$\lim_{n\to\infty} \mathbf{P}_n\big(\mathrm{GCD}_2(\mathbf{N}_D^{(n)}) = A\big) = \prod_{a\in A} \frac{1}{a^D} \prod_{p\in\mathcal{P}(A)} \left(1 - \frac{1}{p^D}\right) \prod_{p\notin\mathcal{P}(A)} \left(1 - \frac{2^D}{p^D}\right). \tag{3.1}$$

For illustration, let us use this to determine the limiting densities of $Z_2^D\big(\mathrm{GCD}_2(\mathbf{N}_D^{(n)})\big)$ in Corollary 1.4 for the value of $r = 2^D - 1$. An interesting corollary is that it allows for the explicit calculation of some infinite series.

Proposition 3.1. *Trivially,* $\mathbf{P}_n\big(Z_2^D\big(\mathrm{GCD}_2(\mathbf{N}_D^{(n)})\big)=2^D\big)=0$ *for all* $n\geq 2$. *Moreover,*

$$\begin{aligned}\lim_{n\to\infty}\mathbf{P}_n\big(Z_2^D\big(\mathrm{GCD}_2(\mathbf{N}_D^{(n)})\big)=2^D-1\big)&=\sum_{a=1}^{\infty}\frac{1}{a^D}\prod_{p\,|\,2a}\Big(1-\frac{1}{p^D}\Big)\prod_{p\nmid 2a}\Big(1-\frac{2^D}{p^D}\Big)\\&=2^D\prod_{p\in\mathcal{P}}\Big(1-\frac{2^D-1}{p^D}\Big).\end{aligned}$$

Remark 3.2. *For* $D=2$, *the fact that the limit equals* $4\prod_{p\in\mathcal{P}}\big(1-3/p^2\big)$ *was already proved in* [5]. *Their result can handle any value of* r *and* M *for* $D=2$. *The proof we provide here is more direct then theirs and with some care the inclusion-exclusion argument here could perhaps be generalised to cover arbitrary* r, M *and* D. *Numerical values of the limit for increasing values of* D *are*

D	2	4	6	8	10
$Z_2^D=2^D-1$	*0.50195*	*0.78874*	*0.90936*	*0.96046*	*0.98257*

Proof. The reason why $Z_2^D\big(\mathrm{GCD}_2(\mathbf{N}_D^{(n)})\big)<2^D$ is that there always exists an index $\mathbf{k}\in\mathcal{W}_2^D$ such that $\gcd(\mathbf{N}_D^{(n)}+\mathbf{k})\geq 2$. If $Z_2^D\big(\mathrm{GCD}_2(\mathbf{N}_D^{(n)})\big)=2^D-1$, then there is precisely one such $\mathbf{k}\in\mathcal{W}_2^D$, moreover, $\gcd(\mathbf{N}_D^{(n)}+\mathbf{k})=2a$ for some $a\in\{1,2,\ldots\}$. Let $B_{\mathbf{k}}(a)$ denote the 2^D-array such that $b_{\mathbf{k}}=2a$ and all other entries are equal to 1. Then of course $\mathcal{P}(B_{\mathbf{k}}(a))=\{p\in\mathcal{P}:\,p\mid 2a\}$. It follows from Corollary 1.4 and (3.1) that

$$\begin{aligned}\lim_{n\to\infty}\mathbf{P}_n\big(Z_2^D\big(\mathrm{GCD}_2(\mathbf{N}_D^{(n)})\big)=2^D-1\big)&=\sum_{a=1}^{\infty}\sum_{\mathbf{k}\in\mathcal{W}_2^D}\mathbf{P}(Z_\infty=B_{\mathbf{k}}(a))\\&=2^D\sum_{a=1}^{\infty}\frac{1}{(2a)^D}\prod_{p\,|\,2a}\Big(1-\frac{1}{p^D}\Big)\prod_{p\nmid 2a}\Big(1-\frac{2^D}{p^D}\Big).\end{aligned}$$

Now let us show the other equality. By definition, for every $\mathbf{k}\in\mathcal{W}_2^D$, the event

$$\big\{\gcd(\mathbf{N}_D^{(n)}+\mathbf{k})=1\big\}=\Big\{(\forall p\in\mathcal{P}_n),\ \min_{1\leq j\leq D}\nu_p(N_j^{(n)}+k_j)=0\Big\}.$$

Let $E_p^{(n)}(\mathbf{k})$ denote the event that $\min_{1\leq j\leq D}\nu_p(N_j^{(n)}+k_j)=0$ and $\overline{F}$ denote the complement of a set F. With this notation,

$$\begin{aligned}\mathbf{P}_n\big(Z_2^D\big(\mathrm{GCD}_2(\mathbf{N}_D^{(n)})\big)=2^D-1\big)&=\mathbf{P}_n\Big(\bigcup_{\mathbf{j}\in\mathcal{W}_2^D}\bigcap_{\mathbf{k}\in\mathcal{W}_2^D\setminus\{\mathbf{j}\}}\gcd(\mathbf{N}_D^{(n)}+\mathbf{k})=1\Big)\\&=\sum_{\mathbf{j}\in\mathcal{W}_2^D}\mathbf{P}_n\Big(\bigcap_{\mathbf{k}\in\mathcal{W}_2^D\setminus\{\mathbf{j}\}}\bigcap_{p\in\mathcal{P}_n}E_p^{(n)}(\mathbf{k})\Big).\end{aligned}\tag{3.2}$$

The probability is independent of the choice of $\mathbf{j}$, therefore, the sum over $\mathcal{W}_2^D$ simply becomes a multiplication by a factor of 2^D. Observe that since $M=2$, the collection of events

$$\big\{\overline{E_p^{(n)}(\mathbf{k})}\big\}_{\mathbf{k}\in\mathcal{W}_2^D}\text{ are mutually exclusive.}$$

This allows for an easy application of De Morgan's law and the inclusion-exclusion principle to deduce that for any $p\in\mathcal{P}$ and subset $W\subseteq\mathcal{W}_2^D$,

$$\mathbf{P}_n\Big(\overline{\bigcap_{\mathbf{k}\in W}E_p^{(n)}(\mathbf{k})}\Big)=\mathbf{P}_n\Big(\bigcup_{\mathbf{k}\in W}\overline{E_p^{(n)}(\mathbf{k})}\Big)=\sum_{\mathbf{k}\in W}\mathbf{P}_n\Big(\overline{E_p^{(n)}(\mathbf{k})}\Big).$$

Hence,

$$\mathbf{P}_n\Big(\bigcap_{\mathbf{k}\in W}E_p^{(n)}(\mathbf{k})\Big)=1-\mathbf{P}_n\Big(\overline{\bigcap_{\mathbf{k}\in W}E_p^{(n)}(\mathbf{k})}\Big)\to 1-\frac{\#W}{p^D}$$

as $n \to \infty$ by an application of (2.1). This can be combined with (3.2) and Proposition 2.1 in a similar fashion as was done in the proof of Theorem 1.2 to complete the proof. □

3.3. **Special case when $M = 3$.** When the side-length of the 'window' is 3, the prime $p = 2$ needs extra attention, otherwise it is similar to the $M = 2$ case. For every $A \in \mathcal{A}_3^D$ we have that $\{2, 3\} \subseteq \mathcal{P}(A)$. Furthermore, for every $p \in \mathcal{P}(A)$ with $p > 2$ we also have that $p \mid a_{\mathbf{k}}$ if and only if $\mathbf{k} = \mathbf{j}_A(p)$. For $p = 2$ the following patterns are possible when $D = 2$:

$$\begin{bmatrix} \checkmark & - & \checkmark \\ - & - & - \\ \checkmark & - & \checkmark \end{bmatrix}, \begin{bmatrix} - & - & - \\ - & \checkmark & - \\ - & - & - \end{bmatrix}, \begin{bmatrix} - & \checkmark & - \\ - & - & - \\ - & \checkmark & - \end{bmatrix}, \begin{bmatrix} - & - & - \\ \checkmark & - & \checkmark \\ - & - & - \end{bmatrix},$$

where ✓ indicates an index which is divisible by 2. In the first one, one of the ✓ is divisible by 4. In the last two cases it is possible that $\#\mathcal{G}_A(2) = 2$, otherwise, $\#\mathcal{G}_A(2) = 1$ always.

Proposition 3.3. *Trivially,* $\mathbf{P}_n\big(Z_3^D\big(\mathrm{GCD}_3(\mathbf{N}_D^{(n)})\big) = 3^D\big) = 0$ *for all* $n \geq 3$. *Furthermore,*

$$\lim_{n\to\infty} \mathbf{P}_n\big(Z_3^D\big(\mathrm{GCD}_3(\mathbf{N}_D^{(n)})\big) = 3^D - 1\big) = \sum_{a=1}^{\infty} \frac{1}{(6a)^D} \prod_{p \mid 6a} \left(1 - \frac{1}{p^D}\right) \prod_{p \nmid 6a} \left(1 - \frac{3^D}{p^D}\right)$$
$$= \frac{1}{6^D} \prod_{p>3} \left(1 - \frac{3^D - 1}{p^D}\right).$$

Sketch of proof. The fact that $\{2, 3\} \subseteq \mathcal{P}(A)$ implies that $\big\{Z_3^D\big(\mathrm{GCD}_3(\mathbf{N}_D^{(n)})\big) = 3^D\big\} = \emptyset$ for all $n \geq 3$. Let $B(a) \in \mathcal{A}_3^D$ be such that $b_{\mathbf{1}} = 6a$ and $b_{\mathbf{k}} = 1$ for $\mathbf{k} \in \mathcal{W}_3^D \setminus \{\mathbf{1}\}$. It is easy to see that

$$Z_3^D\big(\mathrm{GCD}_3(\mathbf{N}_D)\big) = 3^D - 1 \iff \mathrm{GCD}_3(\mathbf{N}_D) = B(a) \text{ for some } a \in \{1, 2, \ldots\}.$$

Hence, Corollary 1.4 implies that

$$\lim_{n\to\infty} \mathbf{P}_n\big(Z_3^D\big(\mathrm{GCD}_3(\mathbf{N}_D^{(n)})\big) = 3^D - 1\big) = \sum_{a=1}^{\infty} \mathbf{P}(Z_\infty = B(a)),$$

which gives the first equality. For the second equality, the $1/6^D$ factor comes from the fact that $6 \mid \mathbf{N}_D^{(n)} + \mathbf{1}$. The primes $p > 3$ can be dealt with in a very similar fashion to the proof of Proposition 3.1 and Theorem 1.2, we leave the details to the interested reader. □

Acknowledgement. IK is supported by the European Research Council Marie Skłodowska-Curie Actions Postdoctoral Fellowship #101109013.

References

[1] E. Cesàro. Sur le plus grand commun diviseur de plusieurs nombres. *Ann. Mat. Pura Appl. (1867-1897)*, 13(3):291–294, 1885.

[2] J. Chidambaraswamy and R. Sitaramachandrarao. On the probability that the values of m polynomials have a given g.c.d. *J. Number Theory*, 26(3):237–245, 1987.

[3] P. G. L. Dirichlet. Über die Bestimmung der mittleren Werthe in der Zahlentheorie. *Abhandlungen der Königlich Preussischen Akademie der Wissenchaften S. 69-83*, pages 49–66, 1849.

[4] J. L. Fernández and P. Fernández. Divisibility properties of random samples of integers. *Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Mat. RACSAM*, 115(26), 2021.

[5] J. L. Fernández and P. Fernández. Counting coprime pairs in random squares. *arXiv e-prints*, 2403.12752v1, 2024.

[6] I. B. Kolossváry and I. T. Kolossváry. Distance between natural numbers based on their prime signature. *J. Number Theory*, 234:120–139, 2022.

[7] E. Kowalski. Arithmetic randonnée: An introduction to probabilistic number theory. https://people.math.ethz.ch/~kowalski/probabilistic-number-theory.pdf, 2021. ETH Zürich Lecture Notes.

HUN-REN Alfréd Rényi Indtitute of Mathematics,
Budapest, Reáltanoda u. 13-15., Hungary
Email address: istvanko@renyi.hu