Bull. Aust. Math. Soc. **93** (2016), 199–210
doi:10.1017/S0004972715001288

ON THE MERTENS–CESÀRO THEOREM FOR NUMBER FIELDS

ANDREA FERRAGUTI and GIACOMO MICHELI✉

(Received 13 June 2015; accepted 4 July 2015; first published online 11 November 2015)

Abstract

Let K be a number field with ring of integers $\mathcal{O}$. After introducing a suitable notion of density for subsets of $\mathcal{O}$, generalising the natural density for subsets of $\mathbb{Z}$, we show that the density of the set of coprime m-tuples of algebraic integers is $1/\zeta_K(m)$, where ζ_K is the Dedekind zeta function of K. This generalises a result found independently by Mertens ['Ueber einige asymptotische Gesetze der Zahlentheorie', *J. reine angew. Math.* **77** (1874), 289–338] and Cesàro ['Question 75 (solution)', *Mathesis* **3** (1883), 224–225] concerning the density of coprime pairs of integers in $\mathbb{Z}$.

2010 *Mathematics subject classification*: primary 11R45; secondary 11R04.

Keywords and phrases: number fields, algebraic integers, natural density, Mertens–Cesàro theorem, zeta function.

1. Introduction

In 1874 Mertens proved that the natural density of the set of coprime pairs of rational integers is $1/\zeta(2)$, where ζ is the Riemann zeta function [8]. In 1881 Cesàro independently asked the same question in [3] and provided the solution two years later in [4], getting the same result as Mertens. Another proof of this result is presented in the book by Hardy and Wright [5, Theorem 330], while a generalisation to the case of m-tuples of integers was given more recently [9].

If one tries to extend the formulation of the theorem to the case of algebraic integers, one encounters some obstructions from the very beginning. In the next paragraphs the reader can find some of the motivations that led to our approach to the problem, especially concerning the definition of the density for a subset of the ring of algebraic integers $\mathcal{O}$ of a number field K.

For the case of the rational integers $\mathbb{Z}$, there exists a 'canonical' way to compute the density of a set $A \subseteq \mathbb{Z}$: this can be defined as the limit in B (if it exists) of the sequence $|A \cap [-B, B)|/(2B)$. This definition extends to the density of a set $A \subseteq \mathbb{Z}^m$ by considering the limit of the sequence $|A \cap [-B, B)^m|/(2B)^m$ as B goes to infinity.

The second author was supported in part by Swiss National Science Foundation grant number 149716 and 161757 and *Armasuisse*.

This definition characterises the probability that, given the m-dimensional hypercube of large side B centred in the origin, a uniformly random selected integer point has all relatively prime entries.

In the setting of algebraic integers, we can consider the analogous problem for the set of m-tuples of ideals of $\mathcal{O}$ using a suitable definition of density involving the norm function. Very interesting results in this direction can be found in [11]. On the other hand, if we want a proper generalisation of the Mertens–Cesàro theorem to $\mathcal{O}$ (and not to the set of ideals of $\mathcal{O}$), the approach presented in [11] does not apply: indeed, given a large bound B, there might be infinitely many elements of norm at most B (contrary to what happens in the case of $\mathbb{Z}$). Therefore, not only does this definition of density for sets of ideals of $\mathcal{O}$ fail to extend to a definition of density for $\mathcal{O}$, but also the analogous probability interpretation that one has over $\mathbb{Z}$ is missing.

A *noncanonical* definition for the density of a subset $A \subseteq \mathcal{O}$ is obtained by considering a $\mathbb{Z}$-isomorphism $\alpha : \mathcal{O} \to \mathbb{Z}^n$ (n being the degree of the extension $K \supseteq \mathbb{Q}$) and then computing the density of $\alpha(A) \subseteq \mathbb{Z}^n$ as previously described. The resulting density is then dependent on the choice of α (that is, equivalent to a choice of a $\mathbb{Z}$-basis for $\mathcal{O}$), but extends to $A \subseteq \mathcal{O}^m$ componentwise, as one would expect by considering the limit of the sequence $|\alpha(A) \cap [-B, B)^{mn}|/(2B)^{mn}$. Using this definition of density for the set $E \subseteq \mathcal{O}^m$ of coprime m-tuples and a similar strategy to the one presented in [7] for the case of unimodular matrices over $\mathbb{Z}$, the following turns out to be true:

- the density d of E can be computed;
- d is *independent* of the choice of the embedding α (that is, independent of the choice of the $\mathbb{Z}$-basis for $\mathcal{O}$);
- $d = 1/\zeta_K(m)$, where $\zeta_K(m)$ is the Dedekind zeta function of the number field K.

This completely generalises the Mertens–Cesàro theorem to the case of number fields. It is very interesting to note that this result matches the one presented in [11, Theorem 4.1], which was obtained in the context of ideals of $\mathcal{O}$.

Outline of the proof. Let us now briefly describe the strategy we use to compute the above-mentioned density in the general case of a subset $E \subseteq \mathbb{Z}^M$ (in our case $M = nm$). First, we find a family $\{E_t\}_{t\in\mathbb{N}}$ of subsets of $\mathbb{Z}^M$ with the following properties:

- we are able to compute the density of E_t for every t (Lemma 3.5);
- $E_{t+1} \subseteq E_t$;
- $\bigcap_{t\in\mathbb{N}} E_t = E$.

Then we verify that the family of sets $\{E_t\}_{t\in\mathbb{N}}$ approximates the set E *in density* in the sense that the sequence of densities of $E_t \backslash E$ converges to zero as $t \to \infty$. Under these assumptions, we are able to prove that $\lim_{t\to\infty} \mathbb{D}(E_t) = \mathbb{D}(E)$ (Theorem 3.7).

1.1. Notation. We say that the ideals $I_1, \dots, I_l$ are coprime if $\sum_j I_j = R$; we say that the elements $a_1, \dots, a_s \in R$ are coprime if the ideals $(a_1), \dots, (a_s)$ are coprime. Let K be a number field of degree n and $\mathcal{O}$ its ring of algebraic integers. Let $\mathbb{E} = \{\mathbf{e}_i\}_{i=1}^n$ be a

$\mathbb{Z}$-basis for $\mathcal{O}$. Define

$$\mathcal{O}[B,\mathbb{E}] = \Big\{\sum_{i=1}^{n} a_i\mathbf{e}_i : a_i \in [-B,B) \cap \mathbb{Z}\Big\}.$$

Later in the paper, we will just write $\mathcal{O}[B]$ since the basis will be understood. For p a prime number, we denote by $S_p = \{\mathfrak{p}_1^{(p)}, \dots, \mathfrak{p}_{\lambda_p}^{(p)}\}$ the set of distinct prime ideals lying over p. In particular, $\prod_{j=1}^{\lambda_p} \mathfrak{p}_j^{(p)}$ is the radical of the ideal generated by p. Let $d_j^{(p)}$ be the inertia degree of $\mathfrak{p}_j^{(p)}$ (that is, $\dim_{\mathbb{F}_p}(\mathcal{O}/\mathfrak{p}_j^{(p)})$) and denote by D_p the integer $\sum_{j=1}^{\lambda_p} d_j^{(p)}$. For d a positive integer, let us denote by $\mathrm{GF}(p,d)$ the finite field of order p^d. Define

$$R_p := \prod_{j=1}^{\lambda_p} \mathcal{O}/\mathfrak{p}_j^{(p)} \cong \prod_{j=1}^{\lambda_p} \mathrm{GF}(p, d_j^{(p)}).$$

For $z = (z_1, \dots, z_m)$ an element of $\mathcal{O}^m$, we denote by I_z the ideal generated by the set $\{z_1, \dots, z_m\}$. If $\mathbb{F}$ is a field, we denote by $\mathbb{F}^*$ its multiplicative group.

2. A definition of the density for $\mathcal{O}^m$

Let $\mathbb{E}$ be a $\mathbb{Z}$-basis for $\mathcal{O}$. Our goal is to define a notion of density (which will in general depend on the choice of $\mathbb{E}$) for a subset T of $\mathcal{O}^m$. We define the *upper density of T with respect to* $\mathbb{E}$ to be

$$\overline{\mathbb{D}}_{\mathbb{E}}(T) = \limsup_{B\to\infty} \frac{|\mathcal{O}[B,\mathbb{E}]^m \cap T|}{(2B)^{mn}}$$

and the *lower density of T with respect to* $\mathbb{E}$ as

$$\underline{\mathbb{D}}_{\mathbb{E}}(T) = \liminf_{B\to\infty} \frac{|\mathcal{O}[B,\mathbb{E}]^m \cap T|}{(2B)^{mn}}.$$

We say that T has *density d with respect to* $\mathbb{E}$ if

$$\overline{\mathbb{D}}_{\mathbb{E}}(T) = \underline{\mathbb{D}}_{\mathbb{E}}(T) =: \mathbb{D}_{\mathbb{E}}(T) = d.$$

Whenever this density is independent of the chosen basis $\mathbb{E}$, it is consistent to denote the density of a set T by $\mathbb{D}(T)$ without any subscript.

Remark 2.1. First, observe that $d \in [0,1] \subseteq \mathbb{R}$ by construction. The main idea behind this definition of density is the same that one has over $\mathbb{Z}$; the only difference is that the way in which we cover the entire set (in this case $\mathcal{O}$) is not canonical but depends on the basis $\mathbb{E}$.

Example 2.2. Let us show with an example that choosing different bases for $\mathcal{O}$ could yield different densities for the same subset $T \subseteq \mathcal{O}$. Let $K = \mathbb{Q}(i)$, so that $\mathcal{O} = \mathbb{Z}[i]$. Let $T = \{x + iy \in \mathcal{O} \colon x, y > 0\}$. If $\mathbb{E} = \{1, i\}$, clearly $|\mathcal{O}[B,\mathbb{E}] \cap T| = (B-1)^2$, which gives $\mathbb{D}_{\mathbb{E}}(T) = 1/4$. On the other hand, choosing as a basis $\mathbb{E}' = \{1, -1+i\} = \{\mathbf{e}_1, \mathbf{e}_2\}$, we have that $T = \{x\mathbf{e}_1 + y\mathbf{e}_2 \in \mathcal{O} \colon x, y > 0,\ x > y\}$. Therefore, $|\mathcal{O}[B,\mathbb{E}'] \cap T| = (B-1)(B-2)/2$, which shows that $\mathbb{D}_{\mathbb{E}'}(T) = 1/8$.

https://doi.org/10.1017/S0004972715001288 Published online by Cambridge University Press

Let $E \subseteq \mathcal{O}^m$ be the set of coprime m-tuples, that is, the elements $z \in \mathcal{O}^m$ for which $I_z = \mathcal{O}$. A corollary of our final result (Theorem 3.7) is that the density of E is actually independent of the basis $\mathbb{E}$: even if the choice of the covering of $\mathcal{O}^m$ is not canonical (it depends in fact on the chosen $\mathbb{Z}$-basis for $\mathcal{O}$) the density of E *is*.

3. Proof of the main result

Let $\mathbb{S}$ be a finite set of prime numbers. Let $E_{\mathbb{S}}$ be the set of m-tuples $z = (z_1, \ldots, z_m)$ in $\mathcal{O}^m$ such that the ideal I_z is coprime with every $p \in \mathbb{S}$.

Remark 3.1. Equivalently, one checks that

$$E_{\mathbb{S}} = \{z \in \mathcal{O}^m : I_z + \mathfrak{p}_j^{(p)} = \mathcal{O} \ \forall p \in \mathbb{S} \text{ and } \forall j \in \{1, \ldots, \lambda_p\}\}$$

by observing that $(p) \subseteq \prod_j \mathfrak{p}_j^{(p)}$ and the $\mathfrak{p}_j^{(p)}$ are maximal.

Let $\psi_p : (\mathcal{O}/(p))^m \to R_p^m = (\prod_{j=1}^{\lambda_p} \mathcal{O}/\mathfrak{p}_j^{(p)})^m$ be the morphism induced by the projection $\mathcal{O}/(p) \twoheadrightarrow \prod_{j=1}^{\lambda_p} \mathcal{O}/\mathfrak{p}_j^{(p)}$. Recall that $D_p = \sum_{j=1}^{\lambda_p} d_j^{(p)}$. In the following lemma and in Proposition 3.3, we will consider the surjection

$$\pi : \mathcal{O}^m \longrightarrow \Big(\prod_{p \in \mathbb{S}} R_p\Big)^m =: T$$

induced by the quotient maps $\mathcal{O} \to \mathcal{O}/\mathfrak{p}_j^{(p)}$. It is easy to prove the following results.

Lemma 3.2. *We have*

$$E_{\mathbb{S}} = \pi^{-1}\Big(\prod_{p \in \mathbb{S}} \prod_{j=1}^{\lambda_p} ((\mathcal{O}/\mathfrak{p}_j^{(p)})^m \setminus \{0\})\Big).$$

Proposition 3.3. *Let q be a positive integer, $\mathbb{E}$ a $\mathbb{Z}$-basis for $\mathcal{O}$, $\mathbb{S}$ a finite set of prime numbers and $N = \prod_{p \in \mathbb{S}} p$. Then*

$$|E_{\mathbb{S}} \cap \mathcal{O}[qN]^m| = (2q)^{mn} \prod_{p \in \mathbb{S}} \Big(p^{nm - mD_p} \prod_{j=1}^{\lambda_p} (p^{d_j^{(p)} m} - 1)\Big),$$

where $\mathcal{O}[qN]^m$ is the set of m-tuples of elements of $\mathcal{O}[qN]$.

Proof. The key point is to decompose the map π. For the rest of the proof, the reader may refer to the following diagram:

$$\begin{array}{ccccc}
\mathcal{O}^m & \xrightarrow{\pi_N} & (\mathcal{O}/(N))^m & \xrightarrow{\overline{\psi}} & T \\
 & & \| & & \| \\
 & & (\prod_{p \in \mathbb{S}} \mathcal{O}/(p))^m & \xrightarrow{\psi} & (\prod_{p \in \mathbb{S}} R_p)^m
\end{array}$$

where π_N is the quotient map and $\psi = (\ldots, \psi_p, \ldots)$ and $\overline{\psi}$ are its obvious extensions to $(\mathcal{O}/(N))^m$ obtained by applying the Chinese remainder theorem to primes in $\mathbb{S}$. Notice then that $\pi = \overline{\psi} \circ \pi_N$. Our strategy to prove the result is to compute the cardinality of the fibres of ψ and the intersection of the fibres of π_N with $\mathcal{O}[qN]$.

For the first, observe that $\psi_p : (\mathcal{O}/(p))^m \to R_p^m$ is a surjective morphism of $\mathbb{F}_p$-vector spaces; therefore, $|\psi_p^{-1}(y_p)| = |\ker(\psi_p)| = p^{nm-mD_p}$ for all $y_p \in R_p^m$. It follows that $|(\overline{\psi})^{-1}(y)| = \prod_{p\in\mathbb{S}} |\psi_p^{-1}(y_p)| = \prod_{p\in\mathbb{S}} p^{nm-mD_p}$ for all $y \in (\mathcal{O}/(N))^m$.

For the second, let $\overline{z} = (\overline{z}_j)_j \in (\mathcal{O}/(N))^m$ and $z = (z_j)_j \in \mathcal{O}^m$. Write

$$\overline{z}_j = \Big(\sum_{t=0}^{n} r_t^j \pi(\mathbf{e}_t)\Big)$$

for some unique $0 \leq r_t^j < N$ in $\mathbb{Z}$. Observe that existence and uniqueness of the r_t^j follow from the fact that $\mathcal{O}/(N)$ is a free $\mathbb{Z}/N\mathbb{Z}$-module of rank n with basis $\{\pi(\mathbf{e}_t)\}$. It follows that $\pi_N(z) = \overline{z}$ if and only if

$$z_j = \sum_{t=0}^{n} (r_t^j + l_t^j N)\mathbf{e}_t$$

for some $l_t^j \in \mathbb{Z}$. We conclude then that

$$|\mathcal{O}[qN]^m \cap \pi_N^{-1}(z)| = (2q)^{mn}$$

since the r_t^j are fixed by the condition $\pi_N(z) = \overline{z}$ and $l_t^j \in [-q, q) \cap \mathbb{Z}$ for each index j, t.

Let us now complete the proof. By Lemma 3.2,

$$E_{\mathbb{S}} \cap \mathcal{O}[qN]^m = \pi^{-1}\Big(\prod_{p\in\mathbb{S}} \prod_{j=1}^{\lambda_p} ((\mathcal{O}/\mathfrak{p}_j^{(p)})^m \backslash \{0\})\Big) \cap \mathcal{O}[qN]^m. \tag{3.1}$$

In order to simplify the notation, define

$$H := \psi^{-1}\Big(\prod_{p\in\mathbb{S}} \prod_{j=1}^{\lambda_p} ((\mathcal{O}/\mathfrak{p}_j^{(p)})^m \backslash \{0\})\Big),$$

so that $E_{\mathbb{S}} = \pi_N^{-1}(H)$ by Lemma 3.2. Since $\pi = \psi \circ \pi_N$, (3.1) reads

$$E_{\mathbb{S}} \cap \mathcal{O}[qN]^m = \pi_N^{-1}(H) \cap \mathcal{O}[qN]^m.$$

Therefore,

$$|\pi_N^{-1}(H) \cap \mathcal{O}[qN]^m| = (2q)^{mn}|H|$$

and

$$|H| = \prod_{p\in\mathbb{S}} \Big(p^{nm-D_p m} \prod_{j=1}^{\lambda_p} |(\mathcal{O}/\mathfrak{p}_j^{(p)})^m \backslash \{0\}|\Big).$$

Thus,

$$|E_{\mathbb{S}} \cap \mathcal{O}[B]| = (2q)^{mn} \prod_{p\in\mathbb{S}} \Big(p^{nm-mD_p} \prod_{j=1}^{\lambda_p} (p^{d_j^{(p)} m} - 1)\Big). \qquad \square$$

https://doi.org/10.1017/S0004972715001288 Published online by Cambridge University Press

Before we proceed, let us recall the following elementary calculus fact.

LEMMA 3.4. *Let $\{a_B\}_{B\in\mathbb{N}}$ be a sequence of real numbers and N a positive integer. Then*

$$\lim_{B\to\infty} a_B = c \Leftrightarrow \lim_{q\to\infty} a_{r+qN} = c \quad \forall r \in \{0,\dots,N-1\}.$$

LEMMA 3.5. *In the notation previously described,*

$$\mathbb{D}(E_{\mathbb{S}}) = \mathbb{D}_{\mathbb{B}}(E_{\mathbb{S}}) = \prod_{p\in\mathbb{S}} \prod_{j=1}^{\lambda_p} \Big(1 - \frac{1}{p^{d_j^{(p)}m}}\Big).$$

PROOF. Let

$$a_B := \frac{|\mathcal{O}[B]^m \cap E_{\mathbb{S}}|}{(2B)^{mn}}.$$

Recall that $N = \prod_{p\in\mathbb{S}} p$. Let

$$D := \prod_{p\in\mathbb{S}} \prod_{j=1}^{\lambda_p} \Big(1 - \frac{1}{p^{d_j^{(p)}m}}\Big).$$

We first show that $a_{qN} = D$. By Proposition 3.3,

$$a_{qN} = \frac{|\mathcal{O}[qN]^m \cap E_{\mathbb{S}}|}{(2qN)^{mn}} = \frac{(2q)^{mn} \prod_{p\in\mathbb{S}} p^{nm-mD_p} \prod_{j=1}^{\lambda_p} (p^{d_j^{(p)}m} - 1)}{(2qN)^{mn}}.$$

Cancelling common factors in numerator and denominator and writing D_p according to its definition gives

$$a_{qN} = \prod_{p\in\mathbb{S}} p^{-m\sum_{j=1}^{\lambda_p} d_j^{(p)}} \prod_{j=1}^{\lambda_p} (p^{d_j^{(p)}m} - 1)$$

and, on bringing $p^{-m\sum_{j=1}^{\lambda_p} d_j^{(p)}}$ inside the products,

$$a_{qN} = \prod_{p\in\mathbb{S}} \prod_{j=1}^{\lambda_p} \Big(1 - \frac{1}{p^{d_j^{(p)}m}}\Big).$$

We are now ready to prove that

$$\lim_{B\to\infty} a_B = D.$$

Thanks to Lemma 3.4, it will be enough to show that

$$\lim_{q\to\infty} a_{r+qN} = D$$

for all $r \in \{0,\dots,N-1\}$. Indeed,

$$a_{qN} \cdot \Big(\frac{2qN}{2r+2qN}\Big)^{mn} < a_{r+qN} < a_{(q+1)N} \cdot \Big(\frac{(2(q+1)N)}{2r+2qN}\Big)^{mn}.$$

By passing to the limit in q the claim follows. □

https://doi.org/10.1017/S0004972715001288 Published online by Cambridge University Press

Remark 3.6. Clearly, the density of $E_{\mathbb{S}}$ is independent of the chosen basis $\mathbb{E}$.

We are now in a position to formulate and prove the main result.

Theorem 3.7. *Let m be a positive integer and K be a number field. Let $\mathcal{O}$ be the ring of integers of K. The density of the set E of coprime m-tuples of $\mathcal{O}$ is*

$$\mathbb{D}(E) = \frac{1}{\zeta_K(m)},$$

where ζ_K is the Dedekind zeta function of the number field K.

Remark 3.8. Let $p_1, \ldots, p_t$ be the first t rational primes. We define $\mathbb{S}_t = \{p_1, \ldots, p_t\}$. The reader should observe that one has the inclusion $E \subseteq E_{\mathbb{S}_t}$ and therefore

$$0 \leq \underline{\mathbb{D}}_{\mathbb{E}}(E) \leq \overline{\mathbb{D}}_{\mathbb{E}}(E) \leq \mathbb{D}(E_{\mathbb{S}_t}).$$

As a consequence, in the case $m = 1$, Theorem 3.7 follows by passing to the limit $t \to \infty$ in the above inequality and recalling that the Dedekind zeta function of K has a pole at 1. As expected in fact, the group of units of the ring of integers has density zero in any basis. Observe that this is the special case $k = 1$ of [2, Corollary 4.2]. A more extensive description of additive representations of elements in the unit group can be found in [1].

Remark 3.9. Notice that the argument of Remark 3.8 does not lead to the conclusion in the case $m > 1$ since it provides just an upper bound (uniform in $\mathbb{E}$) for $\overline{\mathbb{D}}_{\mathbb{E}}(E)$.

Before starting the proof, let us recall the following theorem, which we will use as a fundamental tool.

Theorem 3.10. *Let $S \subseteq \mathbb{R}^M$ be a bounded set whose boundary ∂S can be covered by the images of at most W maps $\phi\colon [0, 1]^{M-1} \to \mathbb{R}^M$ satisfying Lipschitz conditions*

$$|\phi(x) - \phi(y)| \leq L|x - y|$$

for the Euclidean norm. Then S is measurable. Let $V = vol(S)$. Let $\Lambda \subseteq \mathbb{R}^M$ be a full-rank lattice and

$$\lambda_1 := \inf\{|v| \colon v \in \Lambda \backslash \{0\}\}$$

be its first successive minimum. Then

$$\left| |\Lambda \cap S| - \frac{V}{\det \Lambda} \right| \leq cW\left(\frac{L}{\lambda_1} + 1\right)^{M-1}$$

for a constant c depending only on M.

Proof. See [6, Lemma 2]. □

Next we are going to deduce from Theorem 3.10 the particular case that we will use in the proof of Theorem 3.7.

https://doi.org/10.1017/S0004972715001288 Published online by Cambridge University Press

Proposition 3.11. *Let K be a number field of degree n with ring of integers $\mathcal{O}$. Let I be an ideal of $\mathcal{O}$. Then*

$$\left| |(I \cap \mathcal{O}[B])^m| - \frac{(2B)^{nm}}{N(I)^m} \right| \leq c\left(\frac{2B}{c_1 N(I)^{1/n}} + 1\right)^{mn-1}$$

for every $B \in \mathbb{N}$, where $N(I)$ denotes the norm of I and the constants c, c_1 are independent of B and of I.

Proof. Recall that there is a canonical embedding of $\mathcal{O}$ into $\mathbb{R}^n$: if $\sigma_1, \ldots, \sigma_r$ are the real embeddings $K \to \mathbb{R}$ and $\sigma_{r+1}, \ldots, \sigma_{r+2s} = \sigma_n$ are the complex ones labelled such that $\sigma_{r+i} = \overline{\sigma_{r+s+i}}$, then the map $\tau\colon \mathcal{O} \to \mathbb{R}^n$ defined by $x \mapsto (\sigma_1(x), \ldots, \sigma_r(x), \sigma_{r+1}(x), \ldots, \sigma_{r+s}(x))$ embeds $\mathcal{O}$ as a full-rank lattice in $\mathbb{R}^n$, where each σ_{r+i} is thought of as an embedding into $\mathbb{R}^2$. The map τ induces an embedding $\tau^m\colon \mathcal{O}^m \to \mathbb{R}^{mn}$. The image of $\mathcal{O}^m$ inside $\mathbb{R}^{mn}$ via τ^m is again a full-rank lattice. Let $\alpha_{\mathbb{E}} : \mathcal{O} \longrightarrow \mathbb{Z}^n$ be the isomorphism of $\mathbb{Z}$-modules given by $\alpha_{\mathbb{E}}(\sum_{i=1}^n x_i \mathbf{e}_i) = (x_1, \ldots, x_n)$. Let $\alpha_{\mathbb{E}}^m\colon \mathcal{O}^m \to \mathbb{Z}^{mn}$ be the isomorphism induced by $\alpha_{\mathbb{E}}$. Consider the following commutative diagram:

$$\begin{array}{ccc} \mathcal{O}^m & \xrightarrow{\ \tau^m\ } & \mathbb{R}^{mn} \\ \downarrow{\scriptstyle \alpha_{\mathbb{E}}^m} & & \uparrow{\scriptstyle A} \\ \mathbb{Z}^{mn} & \xrightarrow{\ \iota\ } & \mathbb{R}^{mn} \end{array}$$

where ι is the inclusion map and A is the unique $\mathbb{R}$-linear map which makes the diagram commute. The idea now is to apply Theorem 3.10 with $\Lambda = (\iota \circ \alpha_{\mathbb{E}}^m)(I^m) \subseteq \mathbb{R}^{mn}$ and S the cube of side $2B$ centred in the origin, so that $W = 2mn$ and $L = 2B$ in the notation of the theorem. Here by I^m we mean the Cartesian product of m copies of I inside $\mathcal{O}^m$.

We first need a lower bound for the first successive minimum of $(\iota \circ \alpha_{\mathbb{E}}^m)(I^m)$. To do this, we can clearly assume that $m = 1$ since the first successive minimum of a lattice $\Lambda \subseteq \mathbb{R}^n$ coincides with that of $\Lambda^m \subseteq \mathbb{R}^{mn}$. Let v be a vector realising the first successive minimum of $(\iota \circ \alpha_{\mathbb{E}})(I)$ with respect to the Euclidean norm $|\cdot|$. By [6, Lemma 5], the first successive minimum of $\tau(I)$ is greater than or equal to $N(I)^{1/n}$. Since $A(v) \in \tau(I)$,

$$N(I)^{1/n} \leq |A(v)| \leq ||A||\,|v|,$$

where $||A||$ is defined by $\sup_{|w|=1} |A(w)|$. This shows that the first successive minimum of $(\iota \circ \alpha_{\mathbb{E}})(I)$ is greater than or equal to $c_1 N(I)^{1/n}$, where $c_1 := 1/||A||$ is independent of B and of I.

Now the claim follows by applying Theorem 3.10 together with the fact that

$$\det(\alpha_{\mathbb{E}}^m(I^m)) = \det(\alpha_{\mathbb{E}}(I))^m = [\mathbb{Z}^n : \alpha_{\mathbb{E}}(I)]^m = [\mathcal{O}\colon I]^m = N(I)^m$$

and observing that $|(\iota \circ \alpha_{\mathbb{E}}^m)(I^m) \cap [-B, B)^{mn}| = |I^m \cap \mathcal{O}[B]^m| = |(I \cap \mathcal{O}[B])^m|$. □

Proof of Theorem 3.7. We have already proved the theorem in the case $m = 1$ in Remark 3.8; therefore, let us suppose that $m > 1$. Let t be a positive integer, $\mathbb{S}_t$ the

https://doi.org/10.1017/S0004972715001288 Published online by Cambridge University Press

set consisting of the first t prime numbers and define $E_t = E_{\mathbb{S}_t}$. Observe that, since $E_t \supseteq E$,

$$\overline{\mathbb{D}}_{\mathbb{E}}(E) \le \overline{\mathbb{D}}(E_t) = \mathbb{D}(E_t).$$

By letting t run to infinity,

$$\overline{\mathbb{D}}_{\mathbb{E}}(E) \le \frac{1}{\zeta_K(m)}.$$

In order to show the opposite inequality, observe that

$$\mathbb{D}(E_t) - \overline{\mathbb{D}}_{\mathbb{E}}(E_t \backslash E) \le \underline{\mathbb{D}}_{\mathbb{E}}(E). \tag{3.2}$$

Therefore, it is enough to prove that $\lim_{t\to\infty} \overline{\mathbb{D}}_{\mathbb{E}}(E_t \backslash E) = 0$. For a prime ideal $\mathfrak{p} \subseteq \mathcal{O}$, the tth prime number p_t and M an integer, let us introduce the following notation.

- We say that $\mathfrak{p} > M$ if and only if $\mathfrak{p}$ lies over a prime greater than M. (Notice that, with this notation, one has that $\mathfrak{p} > p_t$ implies that $\mathfrak{p} + (p_i) = \mathcal{O}$ for every $i \le t$.)
- We say that $M > \mathfrak{p}$ if and only if the rational prime lying under $\mathfrak{p}$ is less than M.

If $\mathcal{P}$ is the set of prime ideals of $\mathcal{O}$, with this notation,

$$E_t \backslash E \subseteq \bigcup_{\mathfrak{p} \in \mathcal{P} : \mathfrak{p} > p_t} \mathfrak{p}^m \subseteq \mathcal{O}^m,$$

where $\mathfrak{p}^m$ is the set of m-tuples of elements of $\mathcal{O}$ having all entries in $\mathfrak{p}$. It follows that

$$(E_t \backslash E) \cap \mathcal{O}[B]^m \subseteq \bigcup_{\mathfrak{p} \in \mathcal{P} : CB^n > \mathfrak{p} > p_t} (\mathfrak{p} \cap \mathcal{O}[B])^m$$

for C a positive constant independent of B. The upper bound $CB^n > \mathfrak{p}$ comes from the following observation: for a fixed basis $\mathbb{E}$, the norm function is a polynomial of degree n in the coefficients (with respect to the basis $\mathbb{E}$) of the elements of $\mathcal{O}$. Therefore, $N(\mathcal{O}[B]) \subseteq [-CB^n, CB^n]$ for a constant C depending only on the chosen basis. On the other hand, if an element of $\mathcal{O}[B]$ is in $\mathfrak{p}$, then its norm is divisible by the rational prime p lying under $\mathfrak{p}$. This shows that there cannot exist primes $\mathfrak{p} > CB^n$ containing a nonzero element of $\mathcal{O}[B]$. We have then

$$\begin{aligned}\overline{\mathbb{D}}_{\mathbb{E}}(E_t \backslash E) &\le \limsup_{B\to\infty} \Big| \bigcup_{\mathfrak{p} \in \mathcal{P}:\ CB^n > \mathfrak{p} > p_t} \mathfrak{p}^m \cap \mathcal{O}[B]^m \Big| \cdot (2B)^{-nm} \\ &\le \limsup_{B\to\infty} \sum_{\mathfrak{p} \in \mathcal{P}:\ CB^n > \mathfrak{p} > p_t} |\mathfrak{p} \cap \mathcal{O}[B]|^m \cdot (2B)^{-nm}.\end{aligned}$$

By Proposition 3.11,

$$|\mathfrak{p} \cap \mathcal{O}[B]|^m = |(\mathfrak{p} \cap \mathcal{O}[B])^m| \le \frac{(2B)^{mn}}{N(\mathfrak{p})^m} + c\Big(\frac{2B}{c_1 N(\mathfrak{p})^{1/n}} + 1\Big)^{mn-1}.$$

https://doi.org/10.1017/S0004972715001288 Published online by Cambridge University Press

Therefore,

$$\begin{aligned}\overline{\mathbb{D}}_{\mathbb{E}}(E_t\backslash E) &\le \limsup_{B\to\infty} \sum_{CB^n>\mathfrak{p}>p_t} |\mathfrak{p}\cap \mathcal{O}[B]|^m \cdot (2B)^{-nm}\\ &\le \limsup_{B\to\infty} \sum_{CB^n>\mathfrak{p}>p_t} \frac{1}{N(\mathfrak{p})^m} + c\Big(\frac{2B}{c_1 N(\mathfrak{p})^{1/n}}+1\Big)^{mn-1}\cdot (2B)^{-nm}\\ &\le \limsup_{B\to\infty} \sum_{CB^n>p>p_t} \frac{n}{p^m} + cn\Big(\frac{2B}{c_1 p^{1/n}}+1\Big)^{mn-1}\cdot (2B)^{-nm}\\ &=: L_t,\end{aligned}$$

where the last inequality holds because in each instance $N(\mathfrak{p}) \ge p$ for p the prime below $\mathfrak{p}$, and above a fixed rational prime lie at most n distinct primes of $\mathcal{O}$. Now our goal is to show that $L_t \to 0$ as $t \to \infty$.

Choose a constant $c_1' \le c_1$ (independent of B) for which $C^{-1/n} \ge \frac{1}{2}c_1'$. Notice that the sum that appears in L_t is taken over primes p such that $CB^n > p$, whence

$$B > \frac{1}{C^{1/n}} p^{1/n} \ge \frac{c_1'}{2} p^{1/n}.$$

It follows that $2B \ge c_1' p^{1/n}$ and then $2B + c_1' p^{1/n} \le 2\cdot 2B$. Therefore, L_t is bounded by

$$\limsup_{B\to\infty} \sum_{p:CB^n>p>p_t} \frac{n}{p^m} + cn\Big(\frac{4B}{c_1' p^{1/n}}\Big)^{mn-1}\cdot (2B)^{-nm} = \limsup_{B\to\infty} \sum_{p:CB^n>p>p_t} \frac{n}{p^m} + \frac{c'}{Bp^{m-1/n}}$$

for some other constant c' independent of B and p. Now observe that

$$\limsup_{B\to\infty} \sum_{p:CB^n>p>p_t} \frac{n}{p^m} \le \sum_{p>p_t} \frac{n}{p^m}$$

tends to zero when $t \to \infty$ because the series $\sum_p p^{-m}$ is convergent, while

$$\limsup_{B\to\infty} \sum_{CB^n>p>p_t} \frac{c'}{Bp^{m-1/n}} \le \limsup_{B\to\infty} \frac{c'}{B} \sum_{CB^n>p>p_t} \frac{1}{p} = 0$$

since $\sum_{p<CB^n} p^{-1} \sim \log\log(CB^n)$. This concludes the proof by (3.2). □

The following corollary produces the classical generalisation of the Mertens–Cesàro theorem for the case of m-tuples of integers (presented in [9]).

Corollary 3.12 (Extended Mertens–Cesàro theorem). *The density of coprime m-tuples of integers is $1/\zeta(m)$, where ζ is the Riemann zeta function.*

Proof. This follows directly from Theorem 3.7 by setting $K = \mathbb{Q}$. □

Remark 3.13. Observe that the results of Theorem 3.7 are consistent with the expectations. The obtained density is in fact independent of the basis: by symmetry, indeed, all proofs can be done by using another basis $\mathbb{B}$, obtaining the same result.

In addition, Theorem 3.7 extends the Mertens–Cesàro theorem for algebraic integers in the following sense: over $\mathbb{Z}$ one can equivalently consider the density of the set of coprime m-tuples of integers or coprime m-tuples of ideals of $\mathbb{Z}$ without any relevant distinction. If one is willing to do the same in the case of algebraic integers, one has to choose in which context one wants to consider the problem: in the context of m-tuples of ideals, the results in [11] are satisfying while in the setting of m-tuples of algebraic integers, Theorem 3.7 answers the question. Curiously, even if the setup of the problem is very different, the resulting densities match. Future work in this direction could possibly include an analysis of the density of r-prime m-tuples of algebraic integers, extending the definition given by Sittinger in [11].

Remark 3.14. In [10], Schanuel gives an asymptotic for the number of points of bounded height B in the $(m-1)$-dimensional projective space. We will briefly explain why this result goes in a similar direction to the ones in the present note. Let E be the set of coprime m-tuples of $\mathcal{O}_K^m$. There is an action of the group of units $\mathcal{O}_K^*$ on E given by $u(c_1,\dots,c_m) = (uc_1,\dots,uc_m)$ if $u \in \mathcal{O}_K^*$ and $(c_1,\dots,c_m) \in E$. The natural map from E to the $(m-1)$-dimensional projective space $\mathbb{P}_K^{m-1}$ induces an injection ι from $E/\mathcal{O}_K^*$ to $\mathbb{P}_K^{m-1}$. When K has class number one, ι is also a surjection; now one could use [10, Theorem 3] to see that the number of elements of $E/\mathcal{O}_K^*$ of bounded height B is asymptotic to $C_m(K)B^m/\zeta_K(m)$, where $C_m(K)$ is a constant depending on m and the number field K. Schanuel gets the constants because he is essentially 'counting' more objects. For example, when $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, the point $Q = [1+\sqrt{-5}, 2] \in \mathbb{P}_K^1$ would be 'counted' in the case of Schanuel's result even if Q is not proportional to a coprime m-tuple. This happens because the class number of K is different from one.

Acknowledgements

The authors would like to thank Fabrizio Barroero for his suggestion of using Theorem 3.10. We also want to thank Francesco Monopoli and Reto Schnyder for useful comments. Moreover, we are grateful to the anonymous referee for suggestions, which helped us to improve the structure and the content of the paper.

References

[1] F. Barroero, C. Frei and R. Tichy, 'Additive unit representations in rings over global fields – a survey', *Publ. Math. Debrecen* **79**(3) (2011), 291–307.

[2] F. Cellarosi and I. Vinogradov, 'Ergodic properties of k-free integers in number fields', *J. Mod. Dyn.* **7**(3) (2013), 461–488.

[3] E. Cesàro, 'Question proposée 75', *Mathesis* **1** (1881), 184.

[4] E. Cesàro, 'Question 75 (solution)', *Mathesis* **3** (1883), 224–225.

[5] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers* (Clarendon Press, Oxford, 1960).

[6] D. Masser and J. D. Vaaler, 'Counting algebraic numbers with large height II', *Trans. Amer. Math. Soc.* **359**(1) (2007), 427–445.

[7] G. Maze, J. Rosenthal and U. Wagner, 'Natural density of rectangular unimodular integer matrices', *Linear Algebra Appl.* **434**(5) (2011), 1319–1324.

[8] F. Mertens, ‘Ueber einige asymptotische Gesetze der Zahlentheorie’, *J. reine angew. Math.* **77** (1874), 289–338.
[9] J. E. Nymann, ‘On the probability that *k* positive integers are relatively prime’, *J. Number Theory* **4**(5) (1972), 469–473.
[10] S. Schanuel, ‘Heights in number fields’, *Bull. Soc. Math. France* **107**(4) (1979), 433–449.
[11] B. D. Sittinger, ‘The probability that random algebraic integers are relatively *r*-prime’, *J. Number Theory* **130**(1) (2010), 164–171.

ANDREA FERRAGUTI, Institute of Mathematics,
University of Zurich, Winterthurerstrasse 190, 8057 Zurich, Switzerland
e-mail: andrea.ferraguti@math.uzh.ch

GIACOMO MICHELI, Institute of Mathematics,
University of Zurich, Winterthurerstrasse 190, 8057 Zurich, Switzerland
e-mail: giacomo.micheli@math.uzh.ch