John Knopfmacher

Enumerating non-equivalent matrices over principal ideal domains

Mathematica Slovaca, Vol. 44 (1994), No. 3, 287--296

Persistent URL: http://dml.cz/dmlcz/130905

Math. Slovaca, **44** (1994), No. 3, 287–296

Mathematica Slovaca

ENUMERATING NON–EQUIVALENT MATRICES OVER PRINCIPAL IDEAL DOMAINS

JOHN KNOPFMACHER

(*Communicated by Wolfgang Schwarz*)

ABSTRACT. Let $\mathcal{M}_n^\star(R)$ denote the set of all 2-sided equivalence (associate) classes of non-singular $n \times n$ matrices over a given principal ideal domain R. For various domains R arising in algebraic number or function theory, asymptotic estimates are obtained for the average or the total number of classes of large "norm" or "degree" in $\mathcal{M}_n^\star(R)$.

1. Introduction

Let $M_n(R)$ denote the ring of all $n \times n$ matrices with entries in a given principal ideal domain R. In the theory of *integral matrices* (cf. N e w m a n [6]), special attention is frequently paid to the set $\mathcal{M}_n(R)$ of all (2-sided) *equivalence* classes $\bar{A}$ of matrices A in $M_n(R)$, under the relation $\sim$ such that $A \sim B$ if and only if $A = UBV$ for some units U, V in $M_n(R)$.

Usually this is done when R satisfies certain *finite norm* conditions as specified below, and in this paper we shall also confine attention to the subset $\mathcal{M}_n^\star(R)$ of all equivalence classes of *non-singular* matrices in $M_n(R)$.

The *finite norm* conditions to be imposed on R are:

(1.1) for every element $a \neq 0$ in R, the *norm* $N(a) := \operatorname{card}(R/aR) < \infty$;

(1.2) for every integer $k \geq 1$, the total number

$$R(k) := \#\{\text{Non-associate } a \in R:\ N(a) = k\} < \infty .$$

Given condition (1.1), which implies $N(ab) = N(a)N(b)$ by [6; p. 4], it will be useful later to note that (1.2) is then equivalent to:

(1.3) The multiplicative semigroup G_R of all associate classes $\bar{a}$ of non-zero elements $a \in R$ forms an *arithmetical semigroup* in the sense of [2], under the extended norm $N(\bar{a}) := N(a)$.

AMS Subject Classification (1991): Primary 15A33, 15A36, 15A54, 11M41, 11R42, 14G10.

Key words: Equivalence class of matrices, Non-singular matrice, Finit norm condition.

Under the above conditions on R, it is sometimes useful to consider the formal *zeta function*

$$\zeta_R(s) = \sum_{\bar{a}\in G_R} N(\bar{a})^{-s} = \sum_{k=1}^{\infty} R(k)k^{-s}.$$

Now define a *norm* function $\|\ \|$ on $\mathcal{M}_n(R)$ by

$$\|\bar{A}\| = \|A\| = N\big(\det(A)\big),$$

and formally write

$$\zeta_R^{(n)}(s) = \sum_{\bar{A}\in\mathcal{M}_n^\star(R)} \|\bar{A}\|^{-s} = \sum_{k=1}^{\infty} R^{(n)}(k)k^{-s},$$

where

$$R^{(n)}(k) = \#\{\bar{A}\in\mathcal{M}_n^\star(R):\ \|\bar{A}\| = k\}.$$

The *main aim* of this paper is to derive asymptotic estimates for the average $\frac{1}{x}\sum_{k\le x} R^{(n)}(k)$ or for $R^{(n)}(k)$ itself under certain extra assumptions about R, which are always satisfied if R happens also to be

(i) the ring of all algebraic integers in an algebraic number field K, or
(ii) the ring of all integral functions in a given algebraic function field K' in one variable over a finite field $\mathbb{F}_q$,

respectively.

Our arguments will make use of:

(1.4) **Lemma.** *The non-singular matrix zeta function*

$$\zeta_R^{(n)}(s) = \zeta_R(s)\zeta_R(2s)\dots\zeta_R(ns).$$

Proof. By the Smith Normal Form Theorem (cf. [6; p. 26]), every non-singular matrix A in $M_n(R)$ is equivalent to a diagonal matrix of the form

$$S(A) = \operatorname{diag}[a_1, a_1a_2, \dots, a_1a_2\dots a_n],$$

where the $a_i \neq 0$ in R are unique for A up to associates in R. Hence

$$\det(A) = a_1^n a_2^{n-1}\dots a_n.$$

It follows that

$$\begin{aligned}
\zeta_R^{(n)}(s) &= \sum_{k=1}^{\infty} \#\{\bar{A} \in \mathcal{M}_n^\star(R):\ \|\bar{A}\| = k\} k^{-s} \\
&= \sum_{k=1}^{\infty} \#\{(\bar{a}_1, \dots, \bar{a}_n) \in G_R^n:\ N(a_1^n a_2^{n-1} \dots a_n) = k\} k^{-s} \\
&= \Big(\sum_{\bar{a}_1 \in G_R} N(a_1)^{-ns} \Big) \Big(\sum_{\bar{a}_2 \in G_R} N(a_2)^{-(n-1)s} \Big) \cdots \Big(\sum_{\bar{a}_n \in G_R} N(a_n)^{-s} \Big) \\
&= \zeta_R(ns) \zeta_R\big((n-1)s\big) \dots \zeta_R(s)\,,
\end{aligned}$$

recalling the multiplicative property of N and the definition of $\|\ \|$ above.

(1.5) COROLLARY. *When $R = \mathbb{Z}$, the non-singular zeta function for matrices of rational integers*

$$\zeta_{\mathbb{Z}}^{(n)}(s) = \zeta(s)\zeta(2s)\dots\zeta(ns)\,,$$

where $\zeta(s)$ is the Riemann zeta function.

This special case has been used previously by B h o w m i k [1]. We also note two further corollaries:

(1.6) COROLLARY. *If the principal ideal domain R is the ring of all algebraic integers in a given algebraic number field K, then*

$$\zeta_R^{(n)}(s) = \zeta_K(s)\zeta_K(2s)\dots\zeta_K(ns)\,,$$

where $\zeta_K(s)$ is the Dedekind zeta function of K.

(1.7) COROLLARY. *If $R_q = \mathbb{F}_q[t]$ is a polynomial ring in an indeterminate t over the finite field $\mathbb{F}_q$ with q elements, then*

$$\zeta_{R_q}^{(n)}(s) = \prod_{r=1}^{n} \big(1 - q^{1-rs}\big)^{-1}.$$

P r o o f. This corollary is a consequence of Lemma 1.4 and the fact that the special domain $R_q = \mathbb{F}_q[t]$ has zeta function

$$\zeta_{R_q}(s) = \sum_{m=0}^{\infty} q^m \cdot q^{-ms} = \big(1 - q^{1-s}\big)^{-1}.$$

N o t e. Although a theory of generalized, semi-diagonal "Smith normal forms" has been developed for matrices over an arbitrary Dedekind domain R (cf. N a r a n g & N a n d a [5]), this paper will confine attention to the simpler diagonal forms available in the case of a principal ideal domain.

2. Rings of algebraic integers

In this section, it will be *assumed* that the principal ideal domain R is also the ring of all algebraic integers in a given algebraic number field K. We then have:

(2.1) THEOREM. *The numbers*

$$R^{(n)}(k) = \#\{\bar{A} \in \mathcal{M}_n^\star(R) : \ \|\bar{A}\| = k\}$$

have asymptotic mean-value

$$\lim_{x\to\infty} \frac{1}{x} \sum_{k\le x} R^{(n)}(k) = A_K \prod_{r=2}^{n} \zeta_K(r),$$

where $\zeta_K(s)$ is the Dedekind zeta function of K and $A_K > 0$ is a constant. More precisely

$$\sum_{k\le x} R^{(n)}(k) = \left(A_K \prod_{r=\alpha}^{n} \zeta_K(r)\right) x + \rho(x),$$

where

$$\rho(x) = \begin{cases} O(x^\eta) & \text{if } [K:\mathbb{Q}] > 3, \\ O(x^\eta \log x) & \text{if } [K:\mathbb{Q}] = 3, \\ O(\sqrt{x}) & \text{if } [K:\mathbb{Q}] < 3, \end{cases}$$

with $\eta = \eta_K = 1 - 2/(1 + [K:\mathbb{Q}])$.

P r o o f. Under the present assumptions on R, the zeta function

$$\zeta_R(s) = \zeta_K(s) = \sum_{m=1}^{\infty} K(m) m^{-s},$$

where $K(m) = R(m)$ is the number of ideals of index m in R. Then a theorem of Weber and Landau states that

$$\sum_{m\le x} R(m) = \sum_{m\le x} K(m) = A_K x + O(x^\eta),$$

where $A_K > 0$ is an explicit constant (cf. L a n d a u [4]). Furthermore, by some results on isomorphism classes of finite R-modules treated in [2; Chapter 5], the matrix zeta function

$$\zeta_R^{(n)}(s) = \zeta_K(s)\zeta_K(2s)\ldots\zeta_K(ns)$$

can be re-interpreted as the "zeta function" of the category $\mathcal{F}$ of all finite R-modules whose indecomposable direct summands have the form R/P^m for some prime ideal P in R and some $m \leq n$. In order to deduce the present theorem on $\sum_{k \leq x} R^{(n)}(k)$, it is then possible to invoke the following theorem of [2; Chapter 5]:

(**2.2**) **Theorem.** *Let $\alpha = \langle k_1, k_2, \dots \rangle$ be an arbitrary finite or infinite increasing sequence of positive integers, and let $\mathcal{F}^\alpha$ denote the category of all finite R-modules whose indecomposable direct summands have the form R/P^m for some prime ideal P in R and some $m \in \{k_1, k_2, \dots\}$. Let $\mathcal{F}^\alpha(k)$ denote the total number of isomorphism classes of R-modules of cardinal k in $\mathcal{F}^\alpha$. Then the zeta function*

$$\zeta_{\mathcal{F}^\alpha}(s) := \sum_{k=1}^{\infty} \mathcal{F}^\alpha(k) k^{-s} = \prod_{i \geq 1} \zeta_K(k_i s) \qquad \textit{for} \quad \mathrm{Re}(s) \geq k_1^{-1}.$$

Furthermore

$$\sum_{k \leq x} \mathcal{F}^\alpha(k) = \left(A_K \prod_{i \geq 2} \zeta_K(k_i/k_1) \right) x^{1/k_1} + \rho(x),$$

where

$$\rho(x) = \begin{cases} O\left(x^{\eta/k_1}\right) & \textit{if } [K:\mathbb{Q}] > (k_2 + k_1)/(k_2 - k_1), \\ O\left(x^{\varepsilon + k_2^{-1}}\right) & \textit{otherwise } (\varepsilon > 0 \textit{ arbitrary}). \end{cases}$$

In addition, if $k_1 = 1$, then

$$\rho(x) = \begin{cases} O(x^\eta \log x) & \textit{if } [K:\mathbb{Q}] = (k_2 + 1)/(k_2 - 1), \\ O\left(x^{1/k_2}\right) & \textit{if } [K:\mathbb{Q}] < (k_2 + 1)/(k_2 - 1). \end{cases}$$

Theorem 2.1 follows from Theorem 2.2 on consideration of the special sequence $\alpha_n = \langle 1, 2, \dots, n \rangle$ for which $k_1 = 1$, $k_2 = 2$, since the identity $\zeta_R^{(n)}(s) = \zeta_K(s)\zeta_K(2s)\dots\zeta_K(ns)$ then implies that $R^{(n)}(k) = \mathcal{F}^{\alpha_n}(k)$. By way of example, we note that the further special choices $R = \mathbb{Z}$, $\mathbb{Z}[\sqrt{-1}]$ or $\mathbb{Z}[\sqrt{2}]$ yield:

(2.3) Corollary.

(i)

$$\#\left\{\bar{A} \in \mathcal{M}^{\star}(\mathbb{Z}) : |\det(A)| \leq x\right\} = \left(\prod_{r=2}^{n} \zeta(r)\right) x + O(\sqrt{x}),$$

where $\zeta(s)$ is the Riemann zeta function.

(ii)

$$\#\left\{\bar{A} \in \mathcal{M}_n^{\star}(\mathbb{Z}[\sqrt{-1}]) : |\det(A)|^2 \leq x\right\}$$
$$= \left(\frac{\pi}{4} \prod_{r=2}^{n} \zeta_{\sqrt{-1}}(r)\right) x + O(\sqrt{x}).$$

where $\zeta_{\sqrt{-1}}(s)$ is the Dedekind zeta function of $\mathbb{Q}(\sqrt{-1})$.

(iii)

$$\#\left\{\bar{A} \in \mathcal{M}_n^{\star}(\mathbb{Z}[\sqrt{2}]) : N(\det(A)) \leq x\right\}$$
$$= \left(\frac{\log(1+\sqrt{2})}{\sqrt{2}} \prod_{r=2}^{n} \zeta_{\sqrt{2}}(r)\right) x + O(\sqrt{x}).$$

where here $N(a+b\sqrt{2}) = |a^2 - 2b^2|$ $(a, b \in \mathbb{Q})$, and $\zeta_{\sqrt{2}}(s)$ is the Dedekind zeta function of $\mathbb{Q}(\sqrt{2})$.

Remark. With the aid of special estimates involving the Riemann zeta function, Bhowmik [1] has directly given a sharpened version of part (i) of Corollary 2.3.

3. Polynomial and algebraic function rings

Next suppose that the given basic principal ideal domain R is also the principal order in some algebraic function field K' in one variable t over a finite field $\mathbb{F}_q$ with q elements. (The simplest example here is the polynomial ring $R_q = \mathbb{F}_q[t]$ inside $K'_q = \mathbb{F}_q(t)$.)

For a general domain R in the present case, the zeta function $\zeta_R(s)$ takes a simplified form (cf. [3; pp. 13/14], say): Firstly

$$\zeta_R(s) = \sum_{k=1}^{\infty} R(k)k^{-s} = \sum_{m=0}^{\infty} R^{\#}(m)q^{-ms}.$$

where $R^{\#}(m) = R(q^m)$ is the number of associate classes in G_R (or ideals in R) of norm q^m (or *degree* m); here $R(k) = 0$ if k is not a power of q. Secondly, it can be proved that

$$\zeta_R(s) = Z_R(y) = \frac{P(y)}{1 - qy},$$

where $y = q^{-s}$, and $P(y)$ is a polynomial in y with rational integer coefficients. This leads (cf. [3]) to a formula of type

$$R^{\#}(m) = A_R q^m + O(1), \qquad A_R = P(q^{-1}) > 0. \tag{3.1}$$

It now follows that every element $a \neq 0$ in R has the norm of the form $N(a) = q^{\partial(a)}$, where $\partial(a)$ may be called the *degree* of a, and similarly, the norm of an equivalence class $\bar{A} \in \mathcal{M}_n^\star(R)$ may be re-written as

$$\|\bar{A}\| = \|A\| = q^{\partial(\bar{A})} = q^{\partial(A)},$$

where $\partial(\bar{A})$, $\partial(A)$ may be called the q-*degrees* of $\bar{A}$, A respectively (not to be confused with the ordinary degree n of A). In terms of the present notation, we may then re-write $\zeta_R^{(n)}(s) = \zeta_R(s)\zeta_R(2s)\dots\zeta_R(ns)$ in the form

$$\begin{aligned} \zeta_R^{(n)}(s) = Z_R^{(n)}(y) &= \sum_{m=0}^{\infty} R^{(n)}(q^m) y^m \\ &= Z_R(y) Z_R(y^2)\dots Z_R(y^n). \end{aligned} \tag{3.2}$$

Now consider

(3.3) THEOREM. *As* $m \to \infty$

$$R^{(n)}(q^m) = \#\left\{\bar{A} \in \mathcal{M}_n^\star(R) :\ \partial(\bar{A}) = m\right\} = \left(A_R \prod_{r=2}^{n} Z(q^{-r})\right) q^m + O(q^{m/2}).$$

In particular, for $R_q = \mathbb{F}_q[t]$,

$$R_q^{(n)}(q^m) = \left(\prod_{r=1}^{n-1} (1 - q^{-r})\right)^{-1} q^m + O(q^{m/2}).$$

P r o o f. By the formula for $\zeta_{R_q}(s)$ in the proof of Corollary 1.7 above, the second statement follows from the first.

Now, note that $Z_R^{(n)}(y) = F_1(y)$, where $F_i(y) := \prod_{r=i}^{n} Z_R(y^r)$. If $F_2(y) = \sum_{m=0}^{\infty} a_m y^m$, $F_3(y) = \sum_{m=0}^{\infty} b_m y^m$, then the equation $F_2(y) = Z_R(y^2)F_3(y)$ and (3.1) imply that

$$\begin{aligned} |a_m| &= \Big| \sum_{0\le k\le m/2} R^{\#}(k) b_{m-2k} \Big| = O\Big(\sum_{0\le k\le m/2} q^k |b_{m-2k}| \Big) \\ &= O\Big(q^{m/2} \sum_{0\le k} |b_{m-2k}|\, q^{-(m-2k)/2} \Big) = O\big(q^{m/2}\big) \end{aligned}$$

since $F_3\big(q^{-1/2}\big)$ converges absolutely. Thus

$$\sum_{k=0}^{m} a_k q^{-k} = F_2\big(q^{-1}\big) - \sum_{k>m} O\big(q^{-k/2}\big) = F_2(q^{-1}) + O\big(q^{-m/2}\big).$$

It then follows from (3.1) and the equation $F_1(y) = Z_R(y)F_2(y)$ that

$$\begin{aligned} R^{(n)}(q^m) &= \sum_{k=0}^{m} R^{\#}(m-k) a_k = \sum_{k=0}^{m} \big(A_R q^{m-k} + O(1)\big) a_k \\ &= A_R q^m \sum_{k=0}^{m} a_k q^{-k} + O\Big(\sum_{k=0}^{m} q^{k/2} \Big) \\ &= A_R F_2(q^{-1}) q^m + O\big(q^{m/2}\big). \end{aligned}$$

The conclusion of Theorem 3.3 can be considerably sharpened if desired:

(**3.4**) **THEOREM.** *For all sufficiently large m,*

$$R^{(n)}(q^m) = \#\{\bar{A} \in \mathcal{M}_n^{\star}(R) : \ \partial(\bar{A}) = m\} = \sum_{k=1}^{n} \alpha_k(m) q^{m/k}.$$

where

$$\alpha_k(m) = \frac{1}{k} A_R \sum_{h=0}^{k-1} \mathrm{e}^{-2\pi \mathrm{i}\, hm/k} \prod_{\substack{r=1 \\ r\ne k}}^{n} Z_R\big(\mathrm{e}^{2\pi \mathrm{i}\, hr/k} q^{-r/k}\big).$$

In particular, $\alpha_1(m) = A_R \prod_{r=2}^{n} Z_R(q^{-r})$ *as before, and* $\alpha_k(m) = O(1)$ *as* $m \to \infty$.

Proof. The zeta function

$$Z_R^{(n)}(y) = \frac{P(y)}{(1-qy)} \cdot \frac{P(y^2)}{(1-qy^2)} \cdots \frac{P(y^n)}{(1-qy^n)}$$

has a partial fraction decomposition which can be expressed in the form

$$Z_R^{(n)}(y) = Q(y) + \sum_{k=1}^{n} \sum_{h=0}^{k-1} \frac{c(k,h)}{1 - q^{1/k}\, \mathrm{e}^{-2\pi \mathrm{i}\, h/k}\, y},$$

where $Q(y)$ is a polynomial, and $c(k,h)$ is a constant which can be evaluated by l'Hospital's rule:

$$\begin{aligned} c(k,h) &= \lim_{y \to q^{-1/k}\, \mathrm{e}^{2\pi \mathrm{i}\, h/k}} \bigl(1 - q^{1/k}\, \mathrm{e}^{-2\pi \mathrm{i}\, h/k}\, y\bigr) Z_R^{(n)}(y) \\ &= \frac{1}{k} P(q^{-1}) \prod_{\substack{r=1 \\ r \neq k}}^{n} Z_R\bigl(\mathrm{e}^{2\pi \mathrm{i}\, hr/k}\, q^{-r/k}\bigr). \end{aligned}$$

If we now expand $\bigl(1 - q^{1/k}\, \mathrm{e}^{-2\pi \mathrm{i}\, h/k}\, y\bigr)^{-1}$ as a power series within a suitable disc, we obtain

$$\sum_{m=0}^{\infty} R^{(n)}(q^m) y^m = Q(y) + \sum_{m=0}^{\infty} \sum_{k=1}^{n} \sum_{h=0}^{k-1} c(k,h) q^{m/k}\, \mathrm{e}^{-2\pi \mathrm{i}\, mh/k}\, y^m.$$

This leads to the stated formula for $R^{(n)}(q^m)$ when $m > \deg Q(y)$.

(3.5) Corollary. *For $R_q = \mathbb{F}_q[t]$ and any $m \geq 1$,*

$$R_q^{(n)}(q^m) = \sum_{k=1}^{n} \delta_k(m) q^{m/k},$$

where

$$\delta_k(m) = \frac{1}{k} \sum_{h=0}^{k-1} \mathrm{e}^{-2\pi \mathrm{i}\, hm/k} \prod_{\substack{r=1 \\ r \neq k}}^{n} \bigl(1 - \mathrm{e}^{2\pi \mathrm{i}\, hr/k}\, q^{1-r/k}\bigr)^{-1},$$

and $\delta_1(m) = \prod_{r=1}^{n-1} (1 - q^r)^{-1}$ *as before,* $\delta_k(m) = O(1)$ *as* $m \to \infty$.

REFERENCES

[1] BHOWMIK, G.: *Average orders of certain functions connected with arithmetic of matrices*, J. Indian Math. Soc. **60** (1993) (To appear).

[2] KNOPFMACHER, J.: *Abstract Analytic Number Theory*, North-Holland/Dover Publications, Amsterdam-New York, 1975/1990.

[3] KNOPFMACHER, J.: *Analytic Arithmetic of Algebraic Function Fields*, M. Dekker, New York, 1979.

[4] LANDAU, E.: *Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale*, Chelsea Publ. Co., New York, 1949.

[5] NARANG, A.—NANDA, V. C.: *Smith Normal form for matrices over Dedekind domains*, J. Indian Math. Soc. **42** (1978), 173–178.

[6] NEWMAN, M.: *Integral Matrices*, Academic Press, New York, 1972.

Received September 28, 1992

Dept. of Mathematics
University of the Witwatersrand
Johannesburg, P.O. Wits 2050
South Africa