Bull. Aust. Math. Soc. **99** (2019), 56–67
doi:10.1017/S0004972718001090

IDEAL CHAINS IN RESIDUALLY FINITE DEDEKIND DOMAINS

YU-JIE WANG, YI-JING HU and CHUN-GANG JI✉

(Received 14 June 2018; accepted 5 September 2018; first published online 28 November 2018)

Abstract

Let $\mathfrak{D}$ be a residually finite Dedekind domain and let $\mathfrak{n}$ be a nonzero ideal of $\mathfrak{D}$. We consider counting problems for the ideal chains in $\mathfrak{D}/\mathfrak{n}$. By using the Cauchy–Frobenius–Burnside lemma, we also obtain some further extensions of Menon's identity.

2010 *Mathematics subject classification*: primary 11R04; secondary 11B13.

Keywords and phrases: residually finite Dedekind domain, Menon's identity, group action.

1. Introduction

In [3], Menon obtained the identity

$$\sum_{a\in U(\mathbb{Z}/n\mathbb{Z})} \gcd(a-1,n)=\varphi(n)\sigma(n), \tag{1.1}$$

where $\varphi(n)$ is Euler's totient function, $\sigma(n)$ is the divisor function and $U(\mathbb{Z}/n\mathbb{Z})$ denotes the group of units modulo n. In [8], Sury proved the generalisation

$$\sum_{\substack{t_1\in U(\mathbb{Z}/n\mathbb{Z})\\ t_2,\ldots,t_r\in\mathbb{Z}/n\mathbb{Z}}} \gcd(t_1-1,t_2,\ldots,t_r,n)=\varphi(n)\sigma_{r-1}(n),$$

where $\sigma_{r-1}(n)=\sum_{d\mid n} d^{r-1}$. Tărnăuceanu [9] discussed an open problem from [8, Section 2] and Li and Kim [2] extended Tărnăuceanu's results.

Let $\mathfrak{D}$ be a Dedekind domain such that the residue class ring $\mathfrak{D}/\mathfrak{n}$ is finite for each nonzero ideal $\mathfrak{n}$. Then $\mathfrak{D}$ is called a residually finite Dedekind domain. Let $N(\mathfrak{n})=|\mathfrak{D}/\mathfrak{n}|$ be the norm of $\mathfrak{n}$. In [4], Miguel extended the identity (1.1) to residually finite Dedekind domains and obtained the following result.

This work was partially supported by the Grant No. 11471162 from NNSF of China and the Specialized Research Fund for the Doctoral Program of Higher Education of China (Grant No. 20133207110012).

Theorem 1.1 [4]. *Let $\mathfrak{n}$ be a nonzero ideal of $\mathfrak{D}$ and $U(\mathfrak{D}/\mathfrak{n})$ be the multiplicative group of units of $\mathfrak{D}/\mathfrak{n}$. Then*

$$\sum_{a\in U(\mathfrak{D}/\mathfrak{n})} N(\langle a-1\rangle+\mathfrak{n}) = \varphi_{\mathfrak{D}}(\mathfrak{n})\sigma_{\mathfrak{D}}(\mathfrak{n}), \tag{1.2}$$

where $\varphi_{\mathfrak{D}}(\mathfrak{n})$ is the order of the multiplicative group of units in $\mathfrak{D}/\mathfrak{n}$ and $\sigma_{\mathfrak{D}}(\mathfrak{n})$ is the number of ideals that divide $\mathfrak{n}$.

There are some related results in [1, 5, 10]. The key tool in proving these identities is the Cauchy–Frobenius–Burnside lemma (see [7]).

Lemma 1.2 (Cauchy–Frobenius–Burnside lemma). *Let G be a finite group acting on a finite set X and, for each $g \in G$, let $X^g = \{x \in X \mid gx = x\}$ be the set of elements in X that are fixed by g. Denote the set of orbits of X under the action of G by G/X. Then*

$$|G/X| = \frac{1}{|G|}\sum_{g\in G}|X^g|.$$

We give a brief description of the content of this paper. In Sections 2 and 3, we study the counting problems of ideal chains in $\mathfrak{D}/\mathfrak{n}$ by using the group action. In Section 4, we use the *Smith normal form* in a principal ideal domain $\mathfrak{D}_{\mathfrak{p}}$, which is the completion of $\mathfrak{D}$ under a prime ideal $\mathfrak{p}$, to diagonalise the matrices in $\mathfrak{D}$ (Lemma 4.1). As an application, we obtain some new representations of (1.1) and (1.2) (Remarks 4.4 and 4.5). In Sections 5 and 6, we obtain generalisations in residually finite Dedekind domains of the Menon-type identities in [2, 9] (Theorems 5.2 and 6.2).

2. Some lemmas

Let $\mathfrak{D}$ be a residually finite Dedekind domain and let $\mathfrak{n}$ be a nonzero ideal of $\mathfrak{D}$. Then the residue class ring $\mathfrak{D}/\mathfrak{n}$ is a principal ideal ring. It is clear that the mapping

$$\phi : \mathfrak{D} \to \mathfrak{D}/\mathfrak{n}, \quad x \mapsto x+\mathfrak{n}$$

is a surjective ring homomorphism. There is a one-to-one order-preserving correspondence between the ideals $\mathfrak{a}$ of $\mathfrak{D}$ which contain $\mathfrak{n}$ and the ideals $\overline{\mathfrak{a}}$ of $\mathfrak{D}/\mathfrak{n}$, given by $\mathfrak{a} = \phi^{-1}(\overline{\mathfrak{a}})$. We shall use the notation $x \equiv y \pmod{\mathfrak{n}}$, meaning that $x - y \in \mathfrak{n}$.

Let $\mathfrak{n} = \mathfrak{p}_1^{\alpha_1}\cdots\mathfrak{p}_t^{\alpha_t}$, where $\mathfrak{p}_1,\dots,\mathfrak{p}_t$ are distinct prime ideals of $\mathfrak{n}$ and $\alpha_1,\dots,\alpha_t$ are positive integers. By the Chinese remainder theorem, for $i = 1,\dots,t$, there exists $\pi_{\mathfrak{p}_i}$ such that $\pi_{\mathfrak{p}_i} \in \mathfrak{p}_i - \mathfrak{p}_i^2$ and $\pi_{\mathfrak{p}_i} \equiv 1 \pmod{\mathfrak{p}_j}$ for every $j \neq i$. Hence $\overline{\mathfrak{p}}_i = \langle\overline{\pi}_{\mathfrak{p}_i}\rangle$. Without loss of generality, we always take $\overline{\pi}_{\mathfrak{p}_i}$ as the generator of $\overline{\mathfrak{p}}_i$ in $\mathfrak{D}/\mathfrak{n}$. Therefore, we can suppose any ideal $\overline{\mathfrak{a}}$ of $\mathfrak{D}/\mathfrak{n}$ to be of the form

$$\overline{\mathfrak{a}} = \langle\overline{\pi}_{\mathfrak{p}_1}\rangle^{\beta_1}\cdots\langle\overline{\pi}_{\mathfrak{p}_t}\rangle^{\beta_t} = \langle\overline{\eta}_{\mathfrak{a}}\rangle, \tag{2.1}$$

where $0 \leqslant \beta_i \leqslant \alpha_i$ for $i = 1,\dots,t$ and $\eta_{\mathfrak{a}} = \prod_{i=1}^t \pi_{\mathfrak{p}_i}^{\beta_i}$.

Considering the group action of $G = U(\mathfrak{D}/\mathfrak{n})$ on $\mathfrak{D}/\mathfrak{n}$, we define the orbit, $\mathrm{orb}(\overline{\eta})$, of an element $\overline{\eta}$ in $\mathfrak{D}/\mathfrak{n}$ under the action of G by

$$\mathrm{orb}(\overline{\eta}) = \{g\overline{\eta} \mid g \in G\}.$$

In terms of this notation, we can state the following lemma.

https://doi.org/10.1017/S0004972718001090 Published online by Cambridge University Press

LEMMA 2.1. *Let $\mathfrak{n}$ be a nonzero ideal of $\mathfrak{D}$. Then in the principal ideal ring $\mathfrak{D}/\mathfrak{n}$, for every element $\overline{\eta} \in \mathfrak{D}/\mathfrak{n}$, the orbit* $\mathrm{orb}(\overline{\eta})$ *is the set of all generators of the ideal* $\langle\overline{\eta}\rangle$.

Let $\mathfrak{a}$ be an ideal of $\mathfrak{D}$ that contains $\mathfrak{n}$, that is, $\mathfrak{a} \mid \mathfrak{n}$. Let $\overline{\mathfrak{a}} = \langle\overline{\eta}_{\mathfrak{a}}\rangle$. We can define

$$\mathrm{orb}(\overline{\mathfrak{a}}) = \mathrm{orb}(\overline{\eta}_{\mathfrak{a}}). \tag{2.2}$$

LEMMA 2.2. *Let $\mathfrak{a}$ be an ideal of $\mathfrak{D}$ that contains $\mathfrak{n}$. Then*

$$|\mathrm{orb}(\overline{\mathfrak{a}})| = \varphi_{\mathfrak{D}}(\mathfrak{n}/\mathfrak{a}),$$

where $\varphi_{\mathfrak{D}}(\mathfrak{n})$ is the order of the multiplicative group of units in $\mathfrak{D}/\mathfrak{n}$.

PROOF. With the above notation, we can write $\overline{\mathfrak{a}} = \langle\overline{\eta}_{\mathfrak{a}}\rangle$. The stabiliser subgroup of $\overline{\eta}_{\mathfrak{a}}$ in $G = U(\mathfrak{D}/\mathfrak{n})$ is

$$G_{\overline{\eta}_{\mathfrak{a}}} = \{g \in G \mid g\overline{\eta}_{\mathfrak{a}} = \overline{\eta}_{\mathfrak{a}}\}.$$

Here, $g \in G_{\overline{\eta}_{\mathfrak{a}}}$ if and only if $g \in 1 + \mathfrak{n}/\mathfrak{a}$. For the surjective homomorphism

$$\psi : U(\mathfrak{D}/\mathfrak{n}) \to U(\mathfrak{D}/(\mathfrak{n}/\mathfrak{a})),$$

we have $1 + \mathfrak{n}/\mathfrak{a} = \mathrm{Ker}\,\psi$ and $G_{\overline{\eta}_{\mathfrak{a}}} = \mathrm{Ker}\,\psi$. Hence

$$|G_{\overline{\eta}_{\mathfrak{a}}}| = \frac{|U(\mathfrak{D}/\mathfrak{n})|}{|U(\mathfrak{D}/(\mathfrak{n}/\mathfrak{a}))|}.$$

By the orbit-stabiliser theorem and (2.2),

$$|\mathrm{orb}(\overline{\mathfrak{a}})| = |G|/|G_{\overline{\eta}_{\mathfrak{a}}}| = |U(\mathfrak{D}/(\mathfrak{n}/\mathfrak{a}))| = \varphi_{\mathfrak{D}}(\mathfrak{n}/\mathfrak{a}).$$

This completes the proof of Lemma 2.2. □

LEMMA 2.3. *Let $\mathfrak{n}$ be a nonzero ideal of $\mathfrak{D}$ and let $\mathfrak{a}, \mathfrak{b}$ be two ideals of $\mathfrak{D}$ with $\mathfrak{n} \subseteq \mathfrak{b} \subseteq \mathfrak{a} \subseteq \mathfrak{D}$. Then the number of generators of the ideal $\mathfrak{a}/\mathfrak{b}$ in the quotient ring $\mathfrak{D}/\mathfrak{b}$ is $\varphi_{\mathfrak{D}}(\mathfrak{b}/\mathfrak{a})$.*

3. Main results

DEFINITION 3.1. Let $\mathfrak{n}$ be a nonzero ideal of $\mathfrak{D}$ and r be a positive integer. If the ideals $I_1, \ldots, I_r$ of $\mathfrak{D}$ satisfy $\mathfrak{n} \subseteq I_1 \subseteq I_2 \subseteq \cdots \subseteq I_r \subseteq \mathfrak{D}$, then we call $(\overline{I}_1, \ldots, \overline{I}_r)$ an r-ideal chain of the quotient ring $\mathfrak{D}/\mathfrak{n}$. Set $I_0 = \mathfrak{n}$. We define

$$I(\mathfrak{D}/\mathfrak{n}, r) = \{(\overline{I}_1, \ldots, \overline{I}_r) \mid I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots \subseteq I_r \subseteq \mathfrak{D}\}.$$

THEOREM 3.2. *Let $\mathfrak{n}$ be a nonzero ideal of $\mathfrak{D}$ and r be a positive integer. Then*

$$|I(\mathfrak{D}/\mathfrak{n}, r)| = \prod_{\mathfrak{p}^{\alpha} \| \mathfrak{n}} \binom{\alpha + r}{r}.$$

PROOF. Let $\mathfrak{n} = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_t^{\alpha_t}$. Then, by (2.1), all r-ideal chains can be written as

$$0 \subseteq \langle \overline{\pi}_{\mathfrak{p}_1} \rangle^{\alpha_1 - \beta_{11}} \cdots \langle \overline{\pi}_{\mathfrak{p}_t} \rangle^{\alpha_t - \beta_{1t}} \subseteq \cdots \subseteq \langle \overline{\pi}_{\mathfrak{p}_1} \rangle^{\alpha_1 - \beta_{r1}} \cdots \langle \overline{\pi}_{\mathfrak{p}_t} \rangle^{\alpha_t - \beta_{rt}} \subseteq \mathfrak{D}/\mathfrak{n},$$

where $0 \leqslant \beta_{1j} \leqslant \beta_{2j} \leqslant \cdots \leqslant \beta_{rj} \leqslant \alpha_j$ for $j = 1, \ldots, t$. Hence,

$$|I(\mathfrak{D}/\mathfrak{n}, r)| = \sum_{\substack{0 \leqslant \beta_{1j} \leqslant \cdots \leqslant \beta_{rj} \leqslant \alpha_j \\ j=1,\ldots,t}} 1.$$

For $1 \leqslant j \leqslant t$, let

$$\begin{cases} x_{1j} = \beta_{1j} - 0, \\ x_{2j} = \beta_{2j} - \beta_{1j}, \\ \quad \vdots \\ x_{rj} = \beta_{rj} - \beta_{r-1,j}, \\ x_{r+1,j} = \alpha_j - \beta_{rj}. \end{cases} \tag{3.1}$$

Then $x_{ij} \geqslant 0$ for $i = 1, \ldots, r+1$ and $j = 1, \ldots, t$. Hence,

$$|I(\mathfrak{D}/\mathfrak{n}, r)| = \prod_{j=1}^{t} \sum_{\substack{x_{1j} + \cdots + x_{r+1,j} = \alpha_j \\ x_{ij} \geqslant 0, i=1,\ldots,r+1}} 1 = \prod_{j=1}^{t} \binom{\alpha_j + r}{r}.$$

This completes the proof of Theorem 3.2. □

DEFINITION 3.3. Let r be a positive integer and let $\mathfrak{n}$ be a nonzero ideal of $\mathfrak{D}$. For every ideal chain $(\overline{I}_1, \ldots, \overline{I}_r) \in I(\mathfrak{D}/\mathfrak{n}, r)$, we define

$$H(\mathfrak{D}/\mathfrak{n}, \overline{I}_1, \ldots, \overline{I}_r) = \{(x_1, \ldots, x_r) \mid \langle x_i \rangle = I_i/I_{i-1}, x_i \in \mathfrak{D}/I_{i-1}, 1 \leqslant i \leqslant r\}$$

and

$$H(\mathfrak{D}/\mathfrak{n}, r) = \bigcup_{(\overline{I}_1, \ldots, \overline{I}_r) \in I(\mathfrak{D}/\mathfrak{n}, r)} H(\mathfrak{D}/\mathfrak{n}, \overline{I}_1, \ldots \overline{I}_r).$$

THEOREM 3.4. *Let $\mathfrak{n}$ be a nonzero ideal of $\mathfrak{D}$ and r be a positive integer. Then*

$$|H(\mathfrak{D}/\mathfrak{n}, r)| = \varphi_{\mathfrak{D}}^{(r-1)} * I(\mathfrak{n}),$$

where $\varphi_{\mathfrak{D}}^{(r-1)}$ is the $(r-1)$-power of $\varphi_{\mathfrak{D}}$ under the Dirichlet convolution and $I(\mathfrak{n}) = N(\mathfrak{n})$ for a nonzero ideal $\mathfrak{n}$.

PROOF. Let

$$0 \subseteq \overline{I}_1 \subseteq \overline{I}_2 \subseteq \cdots \subseteq \overline{I}_r \subseteq \mathfrak{D}/\mathfrak{n}$$

be an r-ideal chain of $\mathfrak{D}/\mathfrak{n}$, as in Definition 3.1, and let $\mathfrak{n} = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_t^{\alpha_t}$. For $1 \leqslant i \leqslant r$,

$$\overline{I}_i = \langle \overline{\pi}_{\mathfrak{p}_1} \rangle^{\alpha_1 - \beta_{i1}} \cdots \langle \overline{\pi}_{\mathfrak{p}_t} \rangle^{\alpha_t - \beta_{it}}.$$

https://doi.org/10.1017/S0004972718001090 Published online by Cambridge University Press

Hence, by Definition 3.3 and Lemma 2.3,

$$|H(\mathfrak{D}/\mathfrak{n}, \bar{I}_1, \ldots, \bar{I}_r)| = \varphi_{\mathfrak{D}}(\mathfrak{n}/I_1) \cdot \varphi_{\mathfrak{D}}(I_1/I_2) \cdots \varphi_{\mathfrak{D}}(I_{r-1}/I_r)$$
$$= \prod_{j=1}^{t} \varphi_{\mathfrak{D}}(\mathfrak{p}_j^{\beta_{1j}}) \cdot \prod_{j=1}^{t} \varphi_{\mathfrak{D}}(\mathfrak{p}_j^{\beta_{2j}-\beta_{1j}}) \cdots \prod_{j=1}^{t} \varphi_{\mathfrak{D}}(\mathfrak{p}_j^{\beta_{rj}-\beta_{r-1,j}})$$
$$= \prod_{j=1}^{t} \varphi_{\mathfrak{D}}(\mathfrak{p}_j^{\beta_{1j}})\varphi_{\mathfrak{D}}(\mathfrak{p}_j^{\beta_{2j}-\beta_{1j}}) \cdots \varphi_{\mathfrak{D}}(\mathfrak{p}_j^{\beta_{rj}-\beta_{r-1,j}}).$$

Hence,

$$|H(\mathfrak{D}/\mathfrak{n}, r)| = \prod_{j=1}^{t} \sum_{0 \leqslant \beta_{1j} \leqslant \cdots \leqslant \beta_{rj} \leqslant \alpha_j} \varphi_{\mathfrak{D}}(\mathfrak{p}_j^{\beta_{1j}})\varphi_{\mathfrak{D}}(\mathfrak{p}_j^{\beta_{2j}-\beta_{1j}}) \cdots \varphi_{\mathfrak{D}}(\mathfrak{p}_j^{\beta_{rj}-\beta_{r-1,j}}).$$

Define x_{ij} for $1 \leqslant i \leqslant r+1, 1 \leqslant j \leqslant t$ as in (3.1). Since $x_{ij} \geqslant 0$ for $i = 1, \ldots, r+1$ and $j = 1, \ldots, t$,

$$|H(\mathfrak{D}/\mathfrak{n}, r)| = \prod_{j=1}^{t} \sum_{\substack{x_{1j}+\cdots+x_{r+1,j}=\alpha_j \\ x_{ij}\geqslant 0, i=1,\ldots,r+1}} \varphi_{\mathfrak{D}}(\mathfrak{p}_j^{x_{1j}})\varphi_{\mathfrak{D}}(\mathfrak{p}_j^{x_{2j}}) \cdots \varphi_{\mathfrak{D}}(\mathfrak{p}_j^{x_{rj}}).$$

Hence,

$$|H(\mathfrak{D}/\mathfrak{n}, r)| = \prod_{j=1}^{t} \sum_{\mathfrak{p}_j^{x_{1j}} \cdots \mathfrak{p}_j^{x_{rj}} | \mathfrak{p}_j^{\alpha_j}} \varphi_{\mathfrak{D}}(\mathfrak{p}_j^{x_{1j}})\varphi_{\mathfrak{D}}(\mathfrak{p}_j^{x_{2j}}) \cdots \varphi_{\mathfrak{D}}(\mathfrak{p}_j^{x_{rj}})$$
$$= \prod_{j=1}^{t} \sum_{\mathfrak{p}_j^{x_{1j}} \cdots \mathfrak{p}_j^{x_{r-1,j}} | \mathfrak{p}_j^{\alpha_j}} \varphi_{\mathfrak{D}}(\mathfrak{p}_j^{x_{1j}})\varphi_{\mathfrak{D}}(\mathfrak{p}_j^{x_{2j}}) \cdots \varphi_{\mathfrak{D}}(\mathfrak{p}_j^{x_{r-1,j}}) \sum_{\mathfrak{p}_j^{x_{r,j}} | \mathfrak{p}_j^{\alpha_j - x_{1j} - \cdots - x_{r-1,j}}} \varphi_{\mathfrak{D}}(\mathfrak{p}_j^{x_{rj}}).$$

Since $\sum_{i=0}^{\alpha} \varphi_{\mathfrak{D}}(\mathfrak{p}^i) = N(\mathfrak{p})^{\alpha}$,

$$|H(\mathfrak{D}/\mathfrak{n}, r)| = \prod_{j=1}^{t} \sum_{\mathfrak{p}_j^{x_{1j}} \cdots \mathfrak{p}_j^{x_{r-1,j}} | \mathfrak{p}_j^{\alpha_j}} \varphi_{\mathfrak{D}}(\mathfrak{p}_j^{x_{1j}}) \cdots \varphi_{\mathfrak{D}}(\mathfrak{p}_j^{x_{r-1,j}}) N(\mathfrak{p}_j^{\alpha_j}/\mathfrak{p}_j^{x_{1j}} \cdots \mathfrak{p}_j^{x_{r-1,j}})$$
$$= \prod_{j=1}^{t} \varphi_{\mathfrak{D}}^{(r-1)} * I(\mathfrak{p}_j^{\alpha_j}) = \varphi_{\mathfrak{D}}^{(r-1)} * I(\mathfrak{n}).$$

This completes the proof of Theorem 3.4. □

4. Matrix diagonalisation in $M_r(\mathfrak{D}/\mathfrak{n})$

Let K be the field of fractions of $\mathfrak{D}$. From [6, Theorem 3.2, page 90], every discrete valuation v of K is induced by a prime ideal $\mathfrak{p}$ of $\mathfrak{D}$. The completion of K under v will be denoted by $K_{\mathfrak{p}}$ and called the $\mathfrak{p}$-*adic field*, and the ring $\mathfrak{D}_{\mathfrak{p}}$ will be called the ring of integers of $K_{\mathfrak{p}}$. The ring $\mathfrak{D}_{\mathfrak{p}}$ is a Dedekind domain with unique maximal ideal $\mathfrak{p}\mathfrak{D}_{\mathfrak{p}}$. Hence $\mathfrak{D}_{\mathfrak{p}}$ is a principal ideal domain.

https://doi.org/10.1017/S0004972718001090 Published online by Cambridge University Press

Lemma 4.1. *Let $\mathfrak{n}$ be a nonzero ideal of $\mathfrak{D}$ and let $M_r(\mathfrak{D})$ be the set of $r \times r$ matrices with elements in $\mathfrak{D}$. For $A \in M_r(\mathfrak{D})$,*

$$|\{x \in (\mathfrak{D}/\mathfrak{n})^r \mid Ax \equiv 0 \pmod{\mathfrak{n}}\}| = \prod_{\mathfrak{p}^\alpha \| \mathfrak{n}} \prod_{i=1}^{r} N_{\mathfrak{p}}(\langle d_i \rangle + \mathfrak{p}^\alpha),$$

where $d_1, \ldots, d_r$ are all invariant factors of the matrix A in $\mathfrak{D}_{\mathfrak{p}}$ with $d_1 \mid d_2 \mid \cdots \mid d_r$ and $N_{\mathfrak{p}}(\mathfrak{m}) = |\mathfrak{D}_{\mathfrak{p}}/\mathfrak{m}|$. If $d_i = 0$, then $d_{i+1} = \cdots = d_r = 0$ and we define $0 \mid 0$.

Proof. By the Chinese remainder theorem, it is enough to prove the case $\mathfrak{n} = \mathfrak{p}^\alpha$. Since $A \in M_r(\mathfrak{D}) \subseteq M_r(\mathfrak{D}_{\mathfrak{p}})$, according to the Smith normal form over $\mathfrak{D}_{\mathfrak{p}}$, there are two invertible matrices P and $Q \in GL_r(\mathfrak{D}_{\mathfrak{p}})$ such that

$$PAQ = A_{\mathfrak{p}} = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & d_r \end{pmatrix} \in M_r(\mathfrak{D}_{\mathfrak{p}}),$$

where $d_1, \ldots, d_r$ are all invariant factors of A in $\mathfrak{D}_{\mathfrak{p}}$ and $d_1 \mid d_2 \mid \cdots \mid d_r$. If $d_i = 0$, then $d_{i+1} = \cdots = d_r = 0$ and we define $0 \mid 0$.

It is easy to see that the number of solutions of $Ax \equiv 0 \pmod{\mathfrak{p}^\alpha}$ is equal to that of $A_{\mathfrak{p}}x \equiv 0 \pmod{\mathfrak{p}^\alpha}$. By [4, Theorem 2.3], the number of solutions of $Ax \equiv 0 \pmod{\mathfrak{p}^\alpha}$ is

$$\prod_{i=1}^{r} N_{\mathfrak{p}}(\langle d_i \rangle + \mathfrak{p}^\alpha).$$

This completes the proof of Lemma 4.1. □

Denote the set of $r \times r$ invertible matrices in $\mathfrak{D}/\mathfrak{n}$ by $GL_r(\mathfrak{D}/\mathfrak{n})$. Define the set

$$X = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \end{pmatrix} \,\middle|\, x_i \in \mathfrak{D}/\mathfrak{n}, i = 1, \ldots, r \right\}.$$

Definition 4.2. For every invertible matrix $A \in GL_r(\mathfrak{D}/\mathfrak{n})$, we define

$$\varrho_{r,\mathfrak{n}}(A) = |\{x \in X \mid Ax \equiv x \pmod{\mathfrak{n}}\}|.$$

The next theorem is an immediate consequence of Lemma 4.1.

Theorem 4.3. *For every invertible matrix $A \in GL_r(\mathfrak{D}/\mathfrak{n})$,*

$$\varrho_{r,\mathfrak{n}}(A) = \prod_{\mathfrak{p}^\alpha \| \mathfrak{n}} \prod_{i=1}^{r} N_{\mathfrak{p}}(\langle d_i \rangle + \mathfrak{p}^\alpha),$$

where $d_1, \ldots, d_r$ are all invariant factors of the matrix $A - E_r$ in $\mathfrak{D}_{\mathfrak{p}}$ with $d_1 \mid d_2 \mid \cdots \mid d_r$. Here, the matrix E_r stands for the identity matrix of order r.

https://doi.org/10.1017/S0004972718001090 Published online by Cambridge University Press

REMARK 4.4. If $r = 1$, then $A \in U(\mathfrak{D}/\mathfrak{n})$ and $X = \mathfrak{D}/\mathfrak{n}$. For every $a \in U(\mathfrak{D}/\mathfrak{n})$, we shall write $\varrho(a) = \varrho_{1,\mathfrak{n}}(a)$. Then $\varrho(a) = N(\langle a-1\rangle + \mathfrak{n})$. By (1.2),

$$\sum_{a\in U(\mathfrak{D}/\mathfrak{n})} \varrho(a) = \varphi_{\mathfrak{D}}(\mathfrak{n})\sigma_{\mathfrak{D}}(\mathfrak{n}).$$

REMARK 4.5. In particular, let $r = 1$ and $\mathfrak{D} = \mathbb{Z}$. Then, by (1.1),

$$\sum_{a\in U(\mathbb{Z}/n\mathbb{Z})} \varrho(a) = \varphi(n)\sigma(n).$$

5. An application

Let $\mathfrak{D}$ be a residually finite Dedekind domain, let $\mathfrak{n}$ be a nonzero ideal of $\mathfrak{D}$ and let r be a positive integer. Let G denote the group

$$G = \left\{ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1r} \\ 0 & a_{22} & \cdots & a_{2r} \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & a_{rr} \end{pmatrix} \,\middle|\, \begin{array}{l} a_{ii} \in U(\mathfrak{D}/\mathfrak{n}), i = 1, \ldots, r, \\ a_{ij} \in \mathfrak{D}/\mathfrak{n}, 1 \leqslant i < j \leqslant r \end{array} \right\}$$

and let X denote the set

$$X = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \end{pmatrix} \,\middle|\, x_i \in \mathfrak{D}/\mathfrak{n}, i = 1, \ldots, r \right\}.$$

LEMMA 5.1. *Let $\mathfrak{n}$ be a nonzero ideal of $\mathfrak{D}$ and r be a positive integer, and define the group G and the set X as above. Then the number of orbits of X under the action of G is*

$$|G/X| = \prod_{\mathfrak{p}^\alpha \| \mathfrak{n}} \binom{\alpha + r}{r}.$$

PROOF. Two elements x and y of X belong to the same orbit if and only if there exists an element $g \in G$ such that $gx = y$. Let

$$g = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1r} \\ 0 & a_{22} & \cdots & a_{2r} \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & a_{rr} \end{pmatrix} \in G.$$

Then

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1r}x_r \equiv y_1 \pmod{\mathfrak{n}}, \\ a_{22}x_2 + \cdots + a_{2r}x_r \equiv y_2 \pmod{\mathfrak{n}}, \\ \quad\vdots \\ a_{rr}x_r \equiv y_r \pmod{\mathfrak{n}}. \end{cases} \tag{5.1}$$

https://doi.org/10.1017/S0004972718001090 Published online by Cambridge University Press

Consider the system of congruences

$$\begin{cases} \langle x_r\rangle = \langle y_r\rangle & \text{in } \mathfrak{D}/\mathfrak{n}, \\ \langle x_{r-1} + I_1\rangle = \langle y_{r-1} + I_1\rangle & \text{in } \mathfrak{D}/I_1, \\ \quad\vdots & \\ \langle x_1 + I_{r-1}\rangle = \langle y_1 + I_{r-1}\rangle & \text{in } \mathfrak{D}/I_{r-1}, \end{cases} \tag{5.2}$$

where the ideals I_j are given by

$$\begin{aligned} I_1 &= \langle x_r\rangle = \langle y_r\rangle, \\ I_2 &= \langle x_{r-1}, x_r\rangle = \langle y_{r-1}, y_r\rangle, \\ &\ \vdots \\ I_r &= \langle x_1, \dots, x_r\rangle = \langle y_1, \dots, y_r\rangle. \end{aligned}$$

It is easy to see that if $x, y \in X$ are in the same orbit under the action of G, that is, x, y satisfy (5.1), then x, y satisfy (5.2). Conversely, for any r-ideal chain $\overline{I}_1 \subseteq \overline{I}_2 \subseteq \cdots \subseteq \overline{I}_r \subseteq \mathfrak{D}/\mathfrak{n}$, defined as above, there is exactly one orbit of G acting on X. Hence $|G/X|$ is the number of distinct r-ideal chains in $\mathfrak{D}/\mathfrak{n}$. By Theorem 3.2,

$$|G/X| = |I(\mathfrak{D}/\mathfrak{n}, r)| = \prod_{\mathfrak{p}^\alpha \| \mathfrak{n}} \binom{\alpha + r}{r}.$$

This completes the proof of Lemma 5.1. □

Theorem 5.2. *Let r be a positive integer and $\mathfrak{n}$ be a nonzero ideal of $\mathfrak{D}$. Let*

$$G = \left\{ (a_{ij})_{r\times r} \;\middle|\; \begin{array}{l} a_{ii} \in U(\mathfrak{D}/\mathfrak{n}), i = 1, \dots, r, \\ a_{ij} \in \mathfrak{D}/\mathfrak{n}, 1 \leqslant i < j \leqslant r, \\ a_{ij} = 0, 1 \leqslant j < i \leqslant r \end{array} \right\}$$

and define $\varrho_{r,\mathfrak{n}}(A)$ as in Definition 4.2. Then

$$\sum_{A\in G} \varrho_{r,\mathfrak{n}}(A) = N(\mathfrak{n})^{r(r-1)/2} \varphi_{\mathfrak{D}}(\mathfrak{n})^r \prod_{\mathfrak{p}^\alpha \| \mathfrak{n}} \binom{\alpha + r}{r}.$$

Proof. Consider the group action of G on X. By Definition 4.2, for any element $A \in G$,

$$\varrho_{r,\mathfrak{n}}(A) = |\{x \in X \mid Ax \equiv x \pmod{\mathfrak{n}}\}| = |X^A|.$$

Using the Cauchy–Frobenius–Burnside lemma and Lemma 5.1,

$$\sum_{A\in G} \varrho_{r,\mathfrak{n}}(A) = |G| \cdot |G/X| = N(\mathfrak{n})^{r(r-1)/2} \varphi_{\mathfrak{D}}(\mathfrak{n})^r \prod_{\mathfrak{p}^\alpha \| \mathfrak{n}} \binom{\alpha + r}{r}.$$

This completes the proof of Theorem 5.2. □

https://doi.org/10.1017/S0004972718001090 Published online by Cambridge University Press

LEMMA 5.3. *Let* $\mathfrak{n}$ *be a nonzero ideal of* $\mathfrak{D}$ *and* r *be a positive integer. Define* $\tau_1(\mathfrak{n}) = \sigma_{\mathfrak{D}}(\mathfrak{n})$ *and* $\tau_i(\mathfrak{n}) = \sum_{\mathfrak{d}|\mathfrak{n}} \tau_{i-1}(\mathfrak{d})$ *for* $i \geqslant 2$. *Then*

$$\tau_r(\mathfrak{n}) = \prod_{\mathfrak{p}^\alpha \| \mathfrak{n}} \binom{\alpha + r}{r}.$$

PROOF. Let $\mathfrak{n} = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_t^{\alpha_t}$. We shall prove the lemma by induction on r. For $r = 1$,

$$\tau_1(\mathfrak{n}) = \sigma_{\mathfrak{D}}(\mathfrak{n}) = \prod_{\mathfrak{p}^\alpha \| \mathfrak{n}} \binom{\alpha + 1}{1}.$$

Hence the lemma holds for $r = 1$. Assume that the lemma holds for $r = k$, that is,

$$\tau_k(\mathfrak{n}) = \prod_{\mathfrak{p}^\alpha \| \mathfrak{n}} \binom{\alpha + k}{k}.$$

Now we show that the lemma holds for $r = k + 1$. By the induction hypothesis,

$$\begin{aligned}\tau_{k+1}(\mathfrak{n}) &= \sum_{\mathfrak{d}|\mathfrak{n}} \tau_k(\mathfrak{d}) = \sum_{\mathfrak{d}|\mathfrak{n}} \prod_{\mathfrak{p}^\alpha \| \mathfrak{d}} \binom{\alpha + k}{k} \\ &= \sum_{\substack{0 \leqslant \beta_i \leqslant \alpha_i \\ 1 \leqslant i \leqslant t}} \prod_{i=1}^{t} \binom{\beta_i + k}{k} = \prod_{i=1}^{t} \sum_{\beta_i = 0}^{\alpha_i} \binom{\beta_i + k}{k} \\ &= \prod_{i=1}^{t} \binom{\alpha_i + k + 1}{k + 1} = \prod_{\mathfrak{p}^\alpha \| \mathfrak{n}} \binom{\alpha_i + k + 1}{k + 1},\end{aligned}$$

showing that the lemma holds for $r = k + 1$. Thus Lemma 5.3 follows by induction. □

The next theorem follows at once from Theorem 5.2 and Lemma 5.3.

THEOREM 5.4. *For every nonzero ideal* $\mathfrak{n}$ *of* $\mathfrak{D}$ *and a positive integer* r,

$$\sum_{A \in G} \varrho_{r,\mathfrak{n}}(A) = N(\mathfrak{n})^{r(r-1)/2} (\varphi_{\mathfrak{D}}(\mathfrak{n}))^r \tau_r(\mathfrak{n}),$$

where G *is defined as in Theorem 5.2.*

Using Theorem 4.3, we have the following corollary.

COROLLARY 5.5. *For every nonzero ideal* $\mathfrak{n}$ *of* $\mathfrak{D}$ *and a positive integer* r,

$$\sum_{A \in G} \prod_{\mathfrak{p}^\alpha \| \mathfrak{n}} \prod_{i=1}^{r} N(\langle d_i \rangle + \mathfrak{p}^\alpha) = N(\mathfrak{n})^{r(r-1)/2} \varphi_{\mathfrak{D}}(\mathfrak{n})^r \tau_r(\mathfrak{n}),$$

where $d_1, \ldots, d_r$ *are all invariant factors of the matrix* $A - E_r$ *in* $\mathfrak{D}_{\mathfrak{p}}$ *satisfying* $d_1 \mid d_2 \mid \cdots \mid d_r$.

REMARK 5.6. If $\mathfrak{D} = \mathbb{Z}$, then Corollary 5.5 reduces to the main theorem of [9].

https://doi.org/10.1017/S0004972718001090 Published online by Cambridge University Press

6. Another application

In this section, we define the group

$$U = \left\{ \begin{pmatrix} 1 & a_{11} & a_{12} & \cdots & a_{1r} \\ 0 & 1 & a_{22} & \cdots & a_{2r} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \middle| \; a_{ij} \in \mathfrak{D}/\mathfrak{n}, 1 \leqslant i \leqslant j \leqslant r \right\}$$

and consider the action of U on the set

$$X = \left\{ \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_r \end{pmatrix} \middle| \; x_i \in \mathfrak{D}/\mathfrak{n}, i = 0, \ldots, r \right\}.$$

Lemma 6.1. *Let* $\mathfrak{n}$ *be a nonzero ideal of* $\mathfrak{D}$ *and* r *be a positive integer. Then the number of orbits of the set* X *under the action of the group* U *is*

$$|U/X| = \varphi_{\mathfrak{D}}^{(r)} * I(\mathfrak{n}).$$

Proof. If two elements $x, y \in X$ are in the same orbit, then there exists an element $g \in U$ such that $gx = y$. That is,

$$\begin{cases} x_0 + a_{11}x_1 + a_{12}x_2 + \cdots + a_{1r}x_r \equiv y_0 \pmod{\mathfrak{n}}, \\ x_1 + a_{22}x_2 + \cdots + a_{2r}x_r \equiv y_1 \pmod{\mathfrak{n}}, \\ \qquad \vdots \\ x_r \equiv y_r \pmod{\mathfrak{n}}. \end{cases}$$

Consider the system of congruences

$$\begin{cases} \langle x_r \rangle = \langle y_r \rangle & \text{in } \mathfrak{D}/\mathfrak{n}, \\ \langle x_{r-1} + I_1 \rangle = \langle y_{r-1} + I_1 \rangle & \text{in } \mathfrak{D}/I_1, \\ \qquad \vdots \\ \langle x_0 + I_r \rangle = \langle y_0 + I_r \rangle & \text{in } \mathfrak{D}/I_r, \end{cases}$$

with the ideals

$$\begin{aligned} I_1 &= \langle x_r \rangle = \langle y_r \rangle, \\ I_2 &= \langle x_{r-1}, x_r \rangle = \langle y_{r-1}, y_r \rangle, \\ &\;\;\vdots \\ I_{r+1} &= \langle x_0, \ldots, x_r \rangle = \langle y_0, \ldots, y_r \rangle. \end{aligned}$$

Let $\overline{I}_1 \subseteq \overline{I}_2 \subseteq \cdots \subseteq \overline{I}_r \subseteq \overline{I}_{r+1} \subseteq \mathfrak{D}/\mathfrak{n}$ be an $(r+1)$-ideal chain in $I(\mathfrak{D}/\mathfrak{n}, r+1)$. Then, for any vector $(x_1, \ldots, x_{r+1}) \in H(\mathfrak{D}/\mathfrak{n}, \overline{I}_1, \ldots, \overline{I}_{r+1})$, there is exactly one orbit of U acting on X. Hence $|G/X| = |H(\mathfrak{D}/\mathfrak{n}, r+1)|$. By Theorem 3.4, $|U/X| = \varphi_{\mathfrak{D}}^{(r)} * I(\mathfrak{n})$. This completes the proof of Lemma 6.1. □

https://doi.org/10.1017/S0004972718001090 Published online by Cambridge University Press

THEOREM 6.2. *For every nonzero ideal $\mathfrak{n}$ of $\mathfrak{D}$ and a positive integer r,*

$$\sum_{A\in U}\varrho_{r+1,\mathfrak{n}}(A) = N(\mathfrak{n})^{r(r+1)/2}\varphi_{\mathfrak{D}}^{(r)} * I(\mathfrak{n}).$$

PROOF. The theorem can be proved in a similar way to Theorem 5.2 by using the Cauchy–Frobenius–Burnside lemma. □

Using Theorem 4.3, we have the following corollary.

COROLLARY 6.3. *For every nonzero ideal $\mathfrak{n}$ of $\mathfrak{D}$ and a positive integer r,*

$$\sum_{A\in U}\prod_{\mathfrak{p}^\alpha\|\mathfrak{n}}\prod_{i=1}^{r+1}N(\langle d_i\rangle+\mathfrak{p}^\alpha) = N(\mathfrak{n})^{r(r+1)/2}\varphi_{\mathfrak{D}}^{(r)} * I(\mathfrak{n}),$$

where $d_1,\ldots,d_{r+1}$ are all invariant factors of matrix $A - E_{r+1}$ in $\mathfrak{D}_\mathfrak{p}$ satisfying $d_1 \mid d_2 \mid \cdots \mid d_{r+1}$.

REMARK 6.4. If $\mathfrak{D}=\mathbb{Z}$, then Corollary 6.3 reduces to [2, Theorem 3.1].

Acknowledgement

The authors would like to thank the referee for helpful comments and valuable suggestions.

References

[1] Y. Li and D. Kim, 'A Menon-type identity with many tuples of group of units in residually finite Dedekind domains', *J. Number Theory* **175** (2017), 42–50.
[2] Y. Li and D. Kim, 'Menon-type identities derived from actions of subgroups of general linear groups', *J. Number Theory* **179** (2017), 97–112.
[3] P. K. Menon, 'On the sum $\sum(a-1,n)[(a,n)=1]$', *J. Indian Math. Soc.* **29** (1965), 155–163.
[4] C. Miguel, 'Menon's identity in residually finite Dedekind domains', *J. Number Theory* **137** (2014), 179–185.
[5] C. Miguel, 'A Menon-type identity in residually finite Dedekind domains', *J. Number Theory* **164** (2016), 43–51.
[6] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers* (Polish Science Publishers, Warsaw, 1974).
[7] P. Neumann, 'A lemma that is not Burnside's', *Math. Sci.* **4** (1979), 133–141.
[8] B. Sury, 'Some number-theoretic identities from group actions', *Rend. Circ. Mat. Palermo* **58** (2009), 99–108.
[9] M. Tărnăuceanu, 'A generalization of Menon's identity', *J. Number Theory* **132** (2012), 2568–2573.
[10] X. Zhang and C. G. Ji, 'Sums of generators of ideals in residue class ring', *J. Number Theory* **174** (2017), 14–25.

YU-JIE WANG, School of Mathematical Sciences,
Nanjing Normal University, Nanjing 210023, PR China
e-mail: wangyujie9291@126.com

YI-JING HU, School of Mathematical Sciences,
Nanjing Normal University, Nanjing 210023, PR China
e-mail: 853100796@qq.com

CHUN-GANG JI, School of Mathematical Sciences,
Nanjing Normal University, Nanjing 210023, PR China
e-mail: cgji@njnu.edu.cn