INTRODUCTION

Elementary Number Theory is done in the ring $\mathbb{Z}$ of integers. Here one is interested in questions like divisibility which is the same as the solution of the equation

$$a\,x = b \quad \text{(equivalently } x\,a = b\text{)}, \tag{1}$$

diophantine equations including linear diophantine equations, system of equations and arithmetical functions. One is also interested in prime factorization and greatest common divisor (g.c.d.) etc.

These questions have also been considered in a Dedekind domain $\mathcal{O}$.

It may be observed that these questions can also be asked quite meaningfully in structures in which addition and multiplication is not universally defined, but is defined only for elements satisfying certain conditions. One such system is the set $\mathcal{M}$ of all matrices (with entries) in a ring R. Since 1 x 1 - matrices are also included in $\mathcal{M}$, in order to be able to do sensible arithmetic in $\mathcal{M}$, it should already be possible in R. We take R to be a Dedekind domain and tackle some of these problems.

Let $\mathfrak{o}$ be a Dedekind domain, k its field of quotients and let $\mathcal{M}$ be the set of all matrices in $\mathfrak{o}$ (integral matrices). At times, we also deal with matrices in k.

The difficulties one comes across are due to the following:

(i) There is no commutativity of multiplication of matrices,

(ii) The residue class rings $\mathfrak{o}/\mathfrak{a}$ are not necessarily finite, and

(iii) $\mathfrak{o}$ is not always a principal ideal domain (P.I.D).

Over a P.I.D. it is possible to show that in certain contexts, the matrices under consideration can be assumed non-singular, without loss of generality. This breaks down for non-principal ideal domains.(non - P.I.D).

The tools available are:

(a) The theory developed by Siegel [10] , in order to deal with matrices (including singular matrices) in the ring of integers of an algebraic number field.

(b) The theory of modules over Dedekind domains,especially the theorem of Chevalley and Steinitz ([9] , Theorem 81 : 11) which helps reduce some of the problems to the case of generalized diagonal matrices

(i.e. direct sum of matrices of rank 1)

(see [2] and [6]).

(c) The observation that matrices of rank 1 behave almost like elements of σ even over a non-P.I.D., and especially, the observation that a matrix of rank 1 in k is integral if and only if its discriminant is integral.

The consideration of a system of linear diophantine equations already amounts to the consideration of a matrix equation in the form $(x_1 \dots x_n)\ A = (b_1 \dots b_n)$ where $(x_1 \dots x_n)$ and $(b_1 \dots b_n)$ are row matrices. We consider somewhat more generally the matrix equation

$$X\ A = B \tag{2}$$

where (naturally) A and B are matrices with same number of columns.

If (2) has a solution, we say that A is a right divisor of B and write $A \mid B$. (There is of course the corresponding notion of left divisor and the theory would be parallel. In order to avoid confusion, we stick, almost always, to right divisors etc.). The solvability of equation (2) could be

reduced to the solvability of

$$Y\ A\ V = U\ B\ V \qquad (3)$$

where

$$Y = U\ X \qquad (4)$$

provided X can be recovered from (4). This is possible if there exists a matrix $\tilde{U}$ such that $\tilde{U}\ Y = \tilde{U}\ U\ X = X$. One knows from Siegel's theory that primitive reduced matrices U have this property.

How simple can one make U B V with U, V primitive and reduced?

We show (Theorem 2.1.9, Page 10) that the equivalence class U B V, contains a matrix of the form diag $[B_1, \ldots, B_n]$ where B_i are 2 x 2 rank 1 matrices and $\delta(B_i) \mid \delta(B_{i+1})$. (For any matrix A, $\delta(A)$ denotes the discriminant of A, in the sense of Siegel [10]). This matrix we say is in the generalized Smith Normal Form (S.N.F.). We also show that the ideals $\delta(B_i) = \mathfrak{b}_i$ are invariants of the equivalence class. Earlier, using similar ideas, Bhandari and Nanda [2] had obtained generalized S.N.F. invariants of 'ideal matrices'. Here we do it for all matrices in k.

We also introduce for each meaningful value of j, the ideal $\delta_j(B)$ = the g.c.d. of j-rowed minors of B and show that $\delta_j(B) = \prod_{i=1}^{j} \flat_i$. (Corollary 2.2.3, Page 29). This shows that $\delta_1(B)$, $\delta_2(B)$, ... are also invariants of B. Moreover, $\flat_i = \delta_i(B)\ (\delta_{i-1}(B))^{-1}$.

In case (2) has an (integral) solution, $\delta_j(A) \mid \delta_j(B)$. (§ 2.1, Page 28-29). These are therefore a set of necessary conditions for the solvability of (2).

We give three different sets of necessary and sufficient conditions for the solvability of (2). (Theorem 2.3.9, Page 59).

Corollary 2.2.5 (Page 31) gives the S.N.F. invariants of the generalized inverse A^{-1} of any matrix A of rank r, and as a consequence we find the precise denominator of A^{-1} for <u>integral</u> matrices A ; generalizing a result (see 1.16) of Siegel [10] . We also obtain as a consequence of this the sufficient condition $\varpi_r \mid \flat_1$ for solvability of (2).

We also obtain, in terms of the invariants of two matrices A and B, the invariants of

(i) A B in case $\delta(A)$ and $\delta(B)$ are coprime and there is a

common unit between A and B (so that $r = r(A) = r(B)$). (Theorem 2.2.11, Page 34),

(ii) $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ in case $\delta(A)$ and $\delta(B)$ are coprime. (Theorem 2.2.14, Page 40), and

(iii) $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ in case $\mathfrak{m}_r \mid b_1$ (Theorem 2.2.12, Page 38).

The first two of these generalize results of Newman ([7] and [8]). We also prove a result on the invariants $\delta_j \left(\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \right)$ without the assumption of coprimality of $\delta(A)$ and $\delta(B)$ (Theorem 2.2.17, Page 42) and show that (i) and (ii) can be deduced from this, thus providing an alternative method of proving these. The proof of (i) given here uses the invariants $\delta_j(A)$, $\delta_j(B)$ and is more straightforward than that of Newman.

The more general linear diophantine equation

$$X_1 A_1 + \ldots + X_n A_n = B \qquad (5)$$

reduces to (2) with $X = (X_1 \ldots X_n)$ and $A = \begin{pmatrix} A_1 \\ \vdots \\ A_n \end{pmatrix}$. This

reduction would be particularly useful if the invariants of A could be found in terms of those of A_i . This appears hard except in some special cases.

If A_1 and A_2 are matrices with the same number of columns in any ring R, and E denotes the identity matrix, then

$A_1 = (E \quad 0)\begin{pmatrix} A_1 \\ A_2 \end{pmatrix}$ and $A_2 = (0 \quad E)\begin{pmatrix} A_1 \\ A_2 \end{pmatrix}$; and

if $A_i = Z_i D$ then $\begin{pmatrix} A_1 \\ A_2 \end{pmatrix} = \begin{pmatrix} Z_1 \\ Z_2 \end{pmatrix} D$. This shows that

the matrix $\begin{pmatrix} A_1 \\ A_2 \end{pmatrix}$ is a right g.c.d. of A_1 and A_2 . The case $n > 2$ is similar.

This implies that a right g.c.d. of any finite set of n matrices $A_1,\ldots,A_n$ with the same number of columns always exists and is the matrix $A = \begin{pmatrix} A_1 \\ \vdots \\ A_n \end{pmatrix}$. Moreover, (5) has a solution if and only if a right g.c.d. of $A_1, \ldots, A_n$ is a right divisor of B. In particular, a solution of (5) always exists in case A is primitive.

We go back to (2). $X A = X U^{-1} U A$ where U is a primitive and reduced matrix, and U^{-1} denotes the generalized inverse of U. So, it might be useful to look for a simple matrix left equivalent to A. We show that, under certain conditions, there is a generalized triamgular matrix $T = (T_{ij})$ (i.e. $T_{ij} = 0$ for $j > i$ and $r(T_{jj}) = 1$) left equivalent to A. (Theorem 3.1.6, Page 84). Also one may choose T_{ij} in a canonical way to get a unique generalized Hermite normal form (H.N.F.). (Theorem 3.1.9, Page 85 and Theorem 3.1.10, Page 86).

For the proof of Theorem 3.1.9 we develop a sort of Division Algorithm in $\mathcal{M}$. We prove that, under suitable conditions on matrices A and B, we can find matrices Q and R such that $A = Q B + R$. (Lemma 3.1.14, Page 91).

There is yet another set of necessary and sufficient conditions for the solvability of (2) in terms of the S.N.F. invariants of B and H.N.F. invariants of A. (see Theorem 3.2.9, Page 105).

We observe that if the H.N.F. invariants of the g.c.d. of $A_1, \ldots, A_n$ could be determined in terms of the H.N.F. invariants of A_i , this would help. This too appears hard except in some special cases.

We use the H.N.F. in the divisor function d(B) which

we explain a little later.

If $X\,A = B$, then $(X \quad 0)\begin{pmatrix} A \\ C \end{pmatrix} = B$ so that $\begin{pmatrix} A \\ C \end{pmatrix}$ is a divisor of B for all C. Thus, there is considerable arbitrariness in the ranks of divisors. (In fact, there are divisors of all ranks between r(B) and the number of columns of B). Since $r\left(\begin{pmatrix} A \\ C \end{pmatrix}\right) \geq r(A)$, it appears natural to consider divisors of the minimal rank.

A result of Siegel ([10] , Lemma 9) - the proof adapted easily to Dedekind domains by Bhandari in his thesis [1] - shows that given a matrix B in k of rank r, there is an integral matrix E_B of rank r such that $B\,E_B = B$. The matrix E_B is called the (integral) right unit of B. (This is a much deeper result than the existence of a right unit of A in k, used in the theory of generalized inverses by non-number theorists). This shows in particular that each matrix B has a right divisor of unit discriminant; the existence, similarly, of a left unit implies that the matrix B is a right divisor of itself.

We now fix a right unit E_B of B and consider only such divisors of B as are right E_B - reduced.

We show that in case r(B) = 1, the left inequivalent reduced right divisors of B are in one-one correspondence with the ideal divisors of $\delta(B)$. (Theorem 3.2.12, Page 106).

This justifies in case of arbitrary ranks also, the definition d(B) as the number of left inequivalent reduced right divisors of a matrix B.

We show (Theorem 3.2.1 Page 98) that there is a one-one correspondence between the left inequivalent reduced right divisors of B and the reduced divisors in H.N.F. of the S.N.F. of B. Using this theorem, we show (Theorem 3.2.9, Page 104) that d(B) is finite in the case the Dedekind domain $\mathfrak{o}$ satisfies the additional (finiteness) condition:

$$\mathfrak{o}/\mathfrak{a} \text{ is finite for all ideals } \mathfrak{a} \text{ in } \mathfrak{o}. \qquad (6)$$

Consider $T = (T_{ij})$ in H.N.F. Then for $j < i$, T_{ij} belong to a fixed system of remainders modulo T_{jj}. In order to obtain all matrices in H.N.F. with fixed $T_{11}, \ldots, T_{nn}$; therefore, T_{jj} must run over all distinct remainders modulo T_{jj}. We show that since T_{jj} is of rank 1, these remainders are in 1 - 1 correspondence with residues modulo $\delta(T_{jj})$.

The assumption (6) thus implies the finiteness of the

set of all matrices in H.N.F. with fixed T_{11} ,..., T_{nn} .

Combining this with the finiteness of d(B) for B of rank 1, we obtain the result that for B of arbitrary rank also, d(B) is finite if σ satisfies (6). Indeed this way we obtain an upper bound for d(B).(Theorem 3.2.13, Page 106).

At the end of Chapter 3, we consider a few simple matrices and explicitly evaluate d(B).

We also obtain a lower bound for d(B), (Theorem 3.2.13, Page 106), by using the result that for every divisor α of δ(B), there is a right divisor A of B with discriminant α . (Theorem 2.5.1, Page 73).

We make another application of Theorem 2.5.1 to obtain a prime factorization of B in the form $P_1 \ldots P_s$ where $\delta(P_i) = \gamma_i$ and $\delta(B) = \gamma_1 \ldots \gamma_s$. (Theorem 2.5.5, Page 79).

There is one more kind of linear equation

$$X A + B Y = T \qquad (7)$$

(This is different from (5) because of non-commutativity). This equation has also been considered by Newman [8] with $\sigma = \mathbb{Z}$. He uses it to show that in case A and B have coprime determinants

the S.N.F. invariants of $\begin{pmatrix} A & T \\ 0 & B \end{pmatrix}$ are the same as those of $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$. We generalize these results.(Theorem 2.3.16 , Page 64 and Theorem 2.3.18, Page 65).

In the rank 1 case we make two observations:

(i) That the equation (7) can be reduced to an equation of the form (5) with n = 2,and

(ii) That in case T = 0, the number of 'fundamental solutions' is N(g.c.d(δ(A), δ(B))), parallel to the case x a + y b = 0 ; a , b in σ .

In Chapter 2, § 4 , we consider the bilinear diophantine equation

$$X A Y = B \qquad (8)$$

in case B = (b) is a 1 x 1-matrix, so that X is a row and Y is a column matrix. We prove in case r(A) $\geq$ 2,a generalization of a theorem of Frobenius , that there is a solution of (8) if and only if $\delta_1(A) \mid \sigma b$. (Theorem 2.4.1, Page 67). In case B is a single column matrix, we just have a system of independent

bilinear equations and the proof is similar. The case of general Δ is however more complicated.

In case $r(A) = 1$, we show by an example that the theorem of Frobenius has no analogue. (Example 2.4.3, Page 71).