ON SYSTEMS OF LINEAR DIOPHANTINE EQUATIONS

FELIX LAZEBNIK
Department of Mathematical Sciences
University of Delaware, Newark, DE 19716, USA

Introduction Something happened to me recently I would wager has happened to many who read this note. Teaching a new topic, you cannot understand one of the proofs. Your first attempt to fill the gap fails. You look through your books for an answer. Next, you ask colleagues, go to the library, maybe even use the interlibrary loan. All in vain. Then it strikes you that, in fact, you cannot answer an even more basic and seemingly more interesting question. You peruse the books again. They seem to have answers to thousands of strange questions, but not to yours (the most natural one!). At the same time you cannot believe that your question could have been overlooked by generations of mathematicians. Days pass; the agony continues.

Then one day, some way or other, you find the answer. In my case the answer was in a book I already owned. It followed from a theorem I had known for a long time, but I had never thought of this particular application. I must admit, indeed, that this theorem appeared in almost *every* book I had checked, but never with a pointer to this particular application, even as an exercise. Were the authors unaware of the application? Or did it seem to obvious to mention? In any case, here is the story.

In my graduate combinatorics course, a proof of the existence of a design was based on the following question: Given a system of linear equations $A\mathbf{x} = \mathbf{b}$, where $A = (a_{i,j})$ is an $m \times n$ matrix with integer entries, and $\mathbf{b}$ is an $m \times 1$ column vector with integer components, does the system have an *integer* solution, i.e. an $n \times 1$ solution vector $\mathbf{x}$ with integer components? The suggested method ([8], Th. 15.6.5) makes use of "a well–known theorem of van der Waerden":

THEOREM (Van der Waerden). *An integer solution of the system exists if and only if, for every row vector* $\mathbf{v}$ *with rational components such that* $\mathbf{v}A$ *has integer components,* $\mathbf{vb}$ *is an integer.*

I had never seen this theorem, and I was surprised that such a criterion could be useful (which it was!). In trying to prove the theorem, I realized that I did not know *any* good method for resolving a more basic question:

> *How can one tell whether a system of linear diophantine equations has a solution? If solutions exist how can one find any or all of them? (*)*

I could not find this question in any of at least 30 modern texts on abstract algebra or number theory. The place I found it at last was the classical text of van der Waerden [14, Exercise 12.3]. Not for the first time this book contained an answer that I could not find in more recent sources — why hadn't I started with it? (Interestingly, the book contains very few exercises, but this one was there.)

The theory behind the solution is closely related to the famous structure theorem for finitely generated abelian groups, or, more generally, for finitely generated modules over principal ideal domains. Various proofs can be found in many books on abstract algebra, e.g., see [7]. We present

a matrix version of the theorem. Let $\mathbf{Z}$ denote the ring of integers, $M_{m,n}(\mathbf{Z})$, $1 \leq m \leq n$, the ring of all integer $m \times n$ matrices, $SL_k(\mathbf{Z})$ the set of all square $k \times k$ matrices with integer entries and determinant 1 or -1 (**unimodular** matrices). By $D = \mathrm{diag}(d_1, d_2, \ldots, d_m) \in M_{m,n}(\mathbf{Z})$ we denote the diagonal matrix that has an integer d_i in the (i,i) entry, $i = 1, \ldots, m$, and zeros elsewhere. Then we have:

THEOREM 1. *Let $A \in M_{m,n}(\mathbf{Z})$. There exist $L \in SL_m(\mathbf{Z})$ and $R \in SL_n(\mathbf{Z})$ such that*

$$LAR = D = \mathrm{diag}(d_1, d_2, \ldots, d_s, 0, \ldots, 0),$$

where $d_i > 0$, $i = 1, \ldots, s$, and $d_i \mid d_{i+1}$, $i = 1, \ldots, s-1$.

A proof can be found, e.g., in [14] or [7]. The idea is to use elementary operations of rows and columns of A. Matrices L and R correspond to compositions of these operations. Though matrices L and R in Theorem 1 may vary, the matrix D is uniquely defined by A and it is called the **Smith normal form** of A.

Let us note immediately that Theorem 1 can be used to answer question (*). Given $A\mathbf{x} = \mathbf{b}$, rewrite it as $D\mathbf{y} = \mathbf{c}$ with $R\mathbf{y} = \mathbf{x}$, $LAR = D$ and $\mathbf{c} = L\mathbf{b}$. But the solution to the diagonal system $D\mathbf{y} = \mathbf{c}$ is easy. More details and a numerical example are given in the Applications section of this paper.

The question of finding an efficient algorithm for computing the Smith normal form of an integer matrix is not trivial. The direct application of elementary operations of rows and columns does not lead to a polynomial-time algorithm: the integers get too large. For more details, see [11] and [3].

Some history Theorem 1 has an interesting history. Question (*) seems not to have been asked, in full generality, until the mid–19th century. Its particular cases appeared in 1849 -1850 in some number–theoretical studies of Hermite [9, p.164, p.265]. In 1858 Heger [10] formulated conditions for the solvability of $A\mathbf{x} = \mathbf{b}$ in the case where A has full rank (i.e., m) over $\mathbf{Z}$. In 1861, the problem was solved in full generality by H.J.S. Smith [12]. Theorem 1 appeared in a form close to the one above in an 1868 treatise by Frobenius [5] who generalized Heger's theorem [5, p.171-173] and emphasized the unimodularity of the transformations [5, p.194-196].

By then many important results on abelian groups had been discovered. Introduced by Gauss, the concept of an abelian group was developed both in number–theoretical studies of Gauss, Schering, Kronecker, and Dirichlet, and in the studies of elliptic functions and abelian integrals of Gauss, Abel, and Jacobi. Not until 1879 did Frobenius and Stickelberger [6] discover and use explicitly the connection between the theory of finitely generated abelian groups and Smith's theorem. In the same year, Frobenius showed that Smith's theory (extended to matrices over polynomial rings) could be used to classify square matrices over fields, up to similarity. (For further history, see [4] and the Historical Notes in [1].) The story reminds us, in particular, that many basic notions and facts of linear algebra (including module theory) were developed within the context of number theory.

Applications Our first application is related to question (*). It also contains a proof of the aforementioned theorem of van der Waerden. Let $\mathbf{Q}$ denote the field of rational numbers.

PROPOSITION 2. *Let A, L, R, D be as in Theorem 1, $\mathbf{b} \in \mathbf{Z}^n$ and $\mathbf{c} = L\mathbf{b}$. Then the following four statements are equivalent:*

(1) The system of linear equations $A\mathbf{x} = \mathbf{b}$ has an integer solution

(2) The system of linear equations $D\mathbf{y} = \mathbf{c}$ has an integer solution

(3) For every rational vector $\mathbf{u}$ such that $\mathbf{u}A$ is an integer vector, the number $\mathbf{ub}$ is an integer

(4) For every rational vector $\mathbf{v}$ such that $\mathbf{v}D$ is an integer vector, the number $\mathbf{vc}$ is an integer.

Proof. (1) $\iff$ (2): Indeed, $A\mathbf{x} = \mathbf{b} \iff (L^{-1}DR^{-1})\mathbf{x} = \mathbf{b} \iff D(R^{-1}\mathbf{x}) = \mathbf{c} \iff D\mathbf{y} = \mathbf{c}$, where $\mathbf{y} = R^{-1}\mathbf{x}$. Since $R \in SL_m(\mathbf{Z})$, then $R^{-1} \in SL_m(\mathbf{Z})$. Therefore $\mathbf{x} \in \mathbf{Z}^n \iff \mathbf{y} = R^{-1}\mathbf{x} \in \mathbf{Z}^n$.

(3) $\iff$ (4): Indeed, $\mathbf{v}D \in \mathbf{Z}^n \iff \mathbf{v}(LAR) \in \mathbf{Z}^n \iff (\mathbf{v}L)AR \in \mathbf{Z}^n \iff (\mathbf{v}L)A \in \mathbf{Z}^nR^{-1} = \mathbf{Z}^n \iff \mathbf{u}A \in \mathbf{Z}^n$, where $\mathbf{u} = \mathbf{v}L$. Since $L \in SL_n(\mathbf{Z})$, then $\mathbf{u} \in \mathbf{Q}^m \iff \mathbf{v} \in \mathbf{Q}^m$, and, by (3), $\mathbf{ub} \in \mathbf{Z}$. But $\mathbf{ub} \in \mathbf{Z} \iff (\mathbf{v}L)(L^{-1}\mathbf{c}) \in \mathbf{Z} \iff \mathbf{vc} \in \mathbf{Z}$. Therefore (3) implies (4). Reversing the order of the argument, we get $\mathbf{u}A \in \mathbf{Z}^n \iff \mathbf{v}D \in \mathbf{Z}^n$ and $\mathbf{vc} \in \mathbf{Z} \iff \mathbf{ub} \in \mathbf{Z}$. Therefore (4) implies (3).

(2) $\iff$ (4): $D\mathbf{y} = \mathbf{c}$ implies $\mathbf{v}(D\mathbf{y}) = \mathbf{vc}$ for every $\mathbf{v} \in \mathbf{Q}^m$, hence $(\mathbf{v}D)\mathbf{y} = \mathbf{vc}$. If $\mathbf{v}D \in \mathbf{Z}^n$, then $\mathbf{vc} \in \mathbf{Z}$. Thus (2) implies (4). In order to prove that (4) implies (2), first we observe that $\mathbf{c} = (c_1, \ldots, c_s, 0, \ldots, 0)$. For suppose $c_j \neq 0, j > s$. Consider $\mathbf{v} = (0, \ldots, 0, 1/(2c_j), 0, \ldots, 0)$ where $1/(2c_j)$ appears in the j–th position. Since $\mathbf{v}D = \mathbf{0} \in \mathbf{Z}^n$, then by (4) $\mathbf{vc} = 1/2 \in \mathbf{Z}$, and we arrive at a contradiction. Thus $c_j = 0$ for $j > s$. Next, for $i = 1, \ldots, s$, we consider vectors $\mathbf{v_i} = (0, \ldots, 0, 1/d_i, 0, \ldots, 0)$. Since $\mathbf{v_i}D \in \mathbf{Z}^n$, then by (4), $\mathbf{v_ic} \in \mathbf{Z}$ and hence $c_i/d_i \in \mathbf{Z}$. Let $\mathbf{y} = (y_1, \ldots, y_s, 0 \ldots, 0)$, where $y_i = c_i/d_i$, $i = 1, \ldots, s$. Then $\mathbf{y} \in \mathbf{Z}^n$, and $D\mathbf{y} = \mathbf{c}$. ∎

With notations as in Proposition 2, one can reduce the solution of the system $A\mathbf{x} = \mathbf{b}$ to a solution of $D\mathbf{y} = \mathbf{c}$ by performing elementary transformations (over $\mathbf{Z}$) of rows and columns of matrix A augmented by vector $\mathbf{b}$. Matrices L and R can be constructed by multiplying matrices corresponding to these transformations. System $D\mathbf{y} = \mathbf{c}$ has a solution if and only if $c_{s+1} = \ldots = c_m = 0$, and $d_i \mid c_i$ for $i = 1, \ldots, s$. A general solution of $D\mathbf{y} = \mathbf{c}$ can be given in the form $\mathbf{y} = (y_1, \ldots, y_s, t_1 \ldots, t_{m-s})$, where $y_i = c_i/d_i$, $i = 1, \ldots, s$, and $t_1, \ldots, t_{m-s}$ are free integer parameters. Then the general solution of $A\mathbf{x} = \mathbf{b}$ is just $R\mathbf{y}$. Clearly, we may assume that each equation is reduced by the greatest common divisor of the coefficients of the variables.

EXAMPLE. Solve the system of diophantine equations $A\mathbf{x} = \mathbf{b}$, where

$$A = \begin{pmatrix} 2 & 1 & 4 \\ -5 & 2 & 6 \end{pmatrix}, \quad \mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \quad \text{and} \quad \mathbf{b} = \begin{pmatrix} 17 \\ -13 \end{pmatrix}.$$

Solution. Consider a sequence of elementary transformations of rows and columns of A. It is well known that they can be achieved by multiplying A by unimodular matrices. Let us represent the transformation of rows by 2×2 matrices L_i's and the ones of columns by 3×3 matrices R_j's, where

the lower indices reflect the order of multiplications. We consider the following transformations (matrices):

$$R_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad R_2 = \begin{pmatrix} 1 & -2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad R_3 = \begin{pmatrix} 1 & 0 & -4 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad L_4 = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix},$$

$$R_5 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -5 & 1 \end{pmatrix}, \quad R_6 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Let $L = L_4$ and $R = R_1R_2R_3R_5R_6$. Then

$$D = LAR = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 & 4 \\ -5 & 2 & 6 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 \\ 1 & 18 & 32 \\ 0 & -5 & -9 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

$$\text{and} \quad \mathbf{c} = L\mathbf{b} = \begin{pmatrix} 17 \\ -47 \end{pmatrix}.$$

Solving $D\mathbf{y} = \mathbf{c}$, and taking $\mathbf{x} = R\mathbf{y}$, we get

$$\mathbf{x} = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 18 & 32 \\ 0 & -5 & -9 \end{pmatrix} \begin{pmatrix} 17 \\ -47 \\ t_1 \end{pmatrix} = \begin{pmatrix} -47 + 2t_1 \\ -829 + 32t_1 \\ 235 - 9t_1 \end{pmatrix}, \quad t_1 \in \mathbf{Z},$$

and the problem is solved. ■

Another application is concerned with a special instance of the following fundamental question in number theory. Let $\mathbf{Z}[x_1, \ldots, x_t]$ denote the ring of polynomials in t variables with integral coefficients, and let $F(\mathbf{x}) \in \mathbf{Z}[x_1, \ldots, x_t]$. It is clear that if the equation $F(\mathbf{x}) = 0$ has an integer solution, then for any integer $n \geq 1$, the congruence $F(\mathbf{x}) \equiv 0 \pmod{n}$ has a solution. The converse, in general, is false, even for the case of one variable. A simple counterexample is provided by $F(x) = (2x+1)(3x+1)$. To show that $(2x+1)(3x+1) \equiv 0 \pmod{n}$ has a solution, write n in the form $n = 2^a 3^b m$, where $\gcd(m, 2) = \gcd(m, 3) = 1$, and a and b are nonnegative integers. Then use the Chinese Remainder Theorem. For more on the relation between congruences and equations see, e.g., [2]. Nevertheless the following is valid.

PROPOSITION 3. *Let $A \in M_{m,n}(\mathbf{Z})$, and $\mathbf{b} \in \mathbf{Z}^n$. Then the system of linear equations $A\mathbf{x} = \mathbf{b}$ has an integer solution if and only if the corresponding system of congruences $A\mathbf{x} \equiv \mathbf{b} \pmod{n}$ has a solution for every positive integer n.*

Proof. Obviously, the first statement implies the second. Suppose the system of congruences has a solution for every positive integer n. Let $L, R, D, \mathbf{y}$ and $\mathbf{c}$ be as in Proposition 2, and let $N \in \mathbf{Z}$ be such that the transition from $A\mathbf{x} = \mathbf{b}$ to $D\mathbf{y} = \mathbf{c}$ uses integers with absolute values smaller than N. Then for every $n \geq N$, $A\mathbf{x} \equiv \mathbf{b} \pmod{n} \iff D\mathbf{y} \equiv \mathbf{c} \pmod{n} \iff d_i y_i \equiv c_i \pmod{n}$, $i = 1, \ldots, s$. The latter system of congruences is solvable in particular when n is a multiple of d_s.

Since $d_i \mid d_s$ for every i, $1 \leq i \leq s$, this implies $d_i \mid (d_i y_i - c_i)$, hence $d_i \mid c_i$ for all $i = 1, \ldots, s$. Therefore $D\mathbf{y} = \mathbf{c}$ has an integer solution, and so does $A\mathbf{x} = \mathbf{b}$. ■

The following statement allows one easily to compute the index of a subgroup of the additive group $\mathbf{Z}^n$, when the index is finite.

PROPOSITION 4. *Let $f : \mathbf{Z}^n \to \mathbf{Z}^n$ be a $\mathbf{Z}$–linear map and $A \in M_{n,n}(\mathbf{Z})$ be its matrix with respect to some choice of bases. Suppose A has rank n. Then the index of $f(\mathbf{Z}^n)$ in $\mathbf{Z}^n$ is equal to $\mid \det A \mid$.*

Proof. By Theorem 1 we can find two unimodular matrices L and R such that $LAR = D = \mathrm{diag}(d_1, d_2, \ldots, d_n)$. Since A is of rank n, all $d_i \neq 0$. Therefore the abelian group $f(\mathbf{Z}^n) \cong d_1\mathbf{Z} \oplus d_2\mathbf{Z} \oplus \ldots \oplus d_n\mathbf{Z}$, and the order of $\mathbf{Z}^n / f(\mathbf{Z}^n)$ is $\mid d_1 d_2 \cdots d_n \mid = \mid \det D \mid$. Since L and R are unimodular, $\mid \det D \mid = \mid \det A \mid$. ■

EXAMPLE. Let $f : \mathbf{Z}^2 \to \mathbf{Z}^2$ be defined by $f((x, y)) = (28x + 38y, 12x + 16y)$. Choosing both bases to be the standard basis of $\mathbf{Z}^2$, we get $A = \begin{pmatrix} 28 & 12 \\ 38 & 16 \end{pmatrix}$. Therefore the index $[\mathbf{Z}^2 \ : \ f(\mathbf{Z}^2)]$ is equal to $\mid \det A \mid = 8$. The Smith normal form of A is $D = \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix}$, hence $f(\mathbf{Z}^2) \cong 2\mathbf{Z} \oplus 4\mathbf{Z}$.

Our next application is related to Proposition 4. It deals with some basic notions of the geometric number theory. Let $\mathbf{R}$ denote the field of real numbers, and $S = \{\mathbf{s_1}, \ldots, \mathbf{s_m}\}$ be a linearly independent set of vectors in $\mathbf{R}^n$. The additive subgroup $L =< S >$ of $\mathbf{R}^n$ generated by S is called the **lattice** generated by S. A **fundamental domain** $T = T(S)$ of the lattice L is defined as

$$T = \{ \sum_{1 \leq i \leq m} x_i \mathbf{s_i} \ : \ 0 \leq x_i < 1, x_i \in \mathbf{R} \}.$$

The **volume** $v(T)$ of T is defined in the usual way, as the square root of the absolute value of the determinant of an $m \times m$ matrix whose i–th row is the coordinate vector of $\mathbf{s_i}$ in the standard basis. Though T itself depends on a particular set of generators of L, the volume of T does not!

PROPOSITION 5. *Let $S = \{\mathbf{s_1}, \ldots, \mathbf{s_m}\}$ and $U = \{\mathbf{u_1}, \ldots, \mathbf{u_t}\}$ be two sets of linearly independent vectors which generate the same lattice L. Then $m = t$ and $v(T(S)) = v(T(U))$.*

Proof. We leave it to the reader. In case of difficulties, look through [13, pp. 30-33 and pp.168-169]. ■

If one considers A with entries from a field, then by elementary operations of rows and columns, A can be brought to a diagonal form. It is a trivial exercise to check that an elementary row (column) operation preserves the dimensions of both row and column spaces of A. Therefore matrices LAR and A have equal dimensions of their row spaces and equal dimensions of their column spaces. Since the dimensions of row space and column space for a diagonal matrix are equal, we have a proof of the following fundamental result.

PROPOSITION 6. *The dimension of row space of a matrix with entries from a field is equal to the dimension of its column space.* ■

Acknowledgements. References [3], [11], and remarks concerning the algorithmic aspects of finding the Smith normal form of an integer matrix were kindly suggested to the author by an anonymous referee. I am also very grateful to Gary Ebert, Todd Powers, Andrew Woldar, the editor and referees, whose numerous comments substantially improved the original version of this paper.

REFERENCES

1. N. Bourbaki, *Elements of Mathematics: Algebra I, Chapters 1-3*, Hermann, Paris, 1974; N. Bourbaki, *Elements of Mathematics: Algebra II, Chapters 4-7*, Springer-Verlag, Berlin New York, 1989.

2. Z.I. Borevich and I.R. Shafarevitch, *Number Theory*, Academic Press, 1966.

3. T.-W. J. Chou and G. E. Collins, Algorithms for the solution of systems of linear Diophantine equations, *SIAM J. Computing* 11 (1982) 687–708.

4. L.E. Dickson, *History of the Theory of Numbers, Volume 2*, G.E. Stechert & Co., New York, 1934.

5. G. Frobenius, Theorie der linearen Formen mit ganzen Coefficienten, *Jour. für Math.*, 86 (1878) 146–208.

6. G. Frobenius und L. Stickelberger, Über Gruppen von Vertauschbaren Elementen, *J. de Crelle* LXXXVI, (1879) 217

7. N. Jacobson, *Basic Algebra I*, W.H. Freeman and Co.,San Francisco, 1974.

8. M. Hall, Jr., *Combinatorial Theory*, Second Ed., John Wiley & Sons, New York, 1986.

9. Ch. Hermite, *Œuvres, t. I*, Gauthier–Villars, Paris, 1905.

10. I. Heger, Denkschriften Acad. Wiss. Wien (Math. Nat.), 14 II (1858) 1-122.

11. R. Kannan and A. Bachem, Polynomial time algorithms to compute Hermite and Smith normal forms of an integer matrix, *SIAM J. Computing*, 8 (1979) 499–507.

12. H.J.S. Smith, On systems of linear indeterminate equations and congruences, p.367, in *Collected Mathematical Papers*, vol.I, 367–409, Oxford, 1894. (= *Phil.Trans. London*, 151 (1861) 293–326.

13. I. N. Stewart and D. O. Tall, *Algebraic Number Theory*, Second Edition, Chapman and Hall, New York, 1987.

14. B.L. van der Waerden, *Algebra, Volume 2*, Frederick Ungar Publishing Co., New York, 1970.