Reprinted from the MATHEMATICS MAGAZINE
Vol. 48, No. 3, May 1975
pp. 159–163

JACOBI'S SOLUTION OF LINEAR DIOPHANTINE EQUATIONS

M. S. WATERMAN, Idaho State University, Pocatello

1. Introduction. C. G. J. Jacobi's 1869 paper *Über die Auflösung der Gleichung*, $\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = fu$ [1] is a careful treatment of linear Diophantine equations. Although Jacobi's first solution is exactly that used by modern authors such as Niven and Zuckerman [2, p. 94–98], he introduces the beautiful concept of equivalent systems of variables and uses this concept to establish the validity of his solution.

The purpose of this paper is to present the theory of equivalent systems of variables and apply them to linear Diophantine equations. The material on equivalent systems is, we feel, of interest in its own right and, while we try to follow Jacobi as much as possible, some of the work is not to be found in his paper. For example, Proposition 1 and Theorems 2, 3, and 4 do not appear in Jacobi's paper.

This material could compose the basis of an independent study project or take home exam in undergraduate number theory.

2. Equivalent systems of variables. We begin with the basic definition.

DEFINITION 1. *Let* $X = (x_1, x_2, \cdots, x_n)$ *and* $Y = (y_1, y_2, \cdots, y_n)$ *be* $1 \times n$ *vectors of variables. X and Y are said to be equivalent systems of variables if* (1) *each vector is defined in terms of the other by a set of linear equations without constant term and* (2) *the vector X has integer values if and only if Y does. If X and Y are related in this fashion we will write* $X \sim Y$. *If X and Y are not equivalent systems of variables, we will write* $X \nsim Y$.

Of course (1) means that $X = YA$ and $Y = XB$ where A and B are $n \times n$ matrices. It is easy to show that (2) implies these matrices must have integer elements.

Jacobi also has another definition regarding linear systems.

DEFINITION 2. *Suppose X and Y are* $1 \times n$ *vectors of variables and* $X = YA$, $Y = XB$. *Then these two systems of linear equations are called reciprocal systems if* $A = B^{-1}$.

Now we relate the two definitions.

PROPOSITION 1. *Suppose* $X \sim Y$ *with* $X = YA$ *and* $Y = XB$. *Then these equations represent reciprocal systems.*

Proof. We have $X = YA = X(BA)$ so that $X(I-BA) = 0$. Since X is a vector of variables, we fix the index j and let $x_j = 1$ and $x_i = 0$ for all $i \neq j$. This implies the jth row of $I - BA$ is the zero vector, and, since j is arbitrary, $I - BA = 0$. Similarly $I - AB = 0$ so that $A = B^{-1}$.

The next theorem shows that the set of possible matrices in equivalent systems of variables forms the unimodular group (with integer elements).

THEOREM 1. *Let* $X = YA$ *where all* x_i*'s and* y_j*'s are distinct variables and the elements of A are integers. Then* $X \sim Y$ *if and only if* $\det(A) = \pm 1$.

Proof. First assume $X \sim Y$. Then $X = YA$, $Y = XB$, and, by Proposition 1, $A^{-1} = B$. Therefore, A^{-1} must have integer elements. It follows that both $\det A$ and $\det A^{-1}$ must be integers with $(\det A)(\det A^{-1}) = 1$. Therefore, $\det A = \pm 1$.

Next assume $\det A = \pm 1$. Then $Y = XA^{-1}$ where $A^{-1} = (\det A)^{-1}(\operatorname{adj} A) = \pm(\operatorname{adj} A)$ has integer elements.

To see why x_i and y_i must be distinct variables consider

$$(x, t) = (y, t)\begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix}.$$

Now $\det\begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix} = 1$ but the equations cannot hold unless $y = 0$. Therefore, $(x, t) \nsim (y, t)$.

As one would expect $\sim$ is an equivalence relation. The proof is left as an exercise.

THEOREM 2. *$\sim$ is an equivalence relation.*

We now need to define two operations. Let $X = (x_1, x_2, \cdots, x_n)$ and $Z = (z_1, z_2, \cdots, z_n)$. Define $X \vee Z = (x_1, x_2, \cdots, x_n, z_1, z_2, \cdots, z_n)$. Also, let $X \ominus Z$ be the vector of all x variables which are not also Z variables. The next results study $\sim$ under these operations.

THEOREM 3. *If $X_1 \sim Y_1$ and $X_2 \sim Y_2$, then $X_1 \vee X_2 \sim Y_1 \vee Y_2$.*

Proof. If $X_1 = A_1 Y_1$ and $X_2 = A_2 Y_2$, then

$$X_1 \vee X_2 = (Y_1 \vee Y_2)\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}.$$

The other equality follows in the same manner.

THEOREM 4. *Let $X_1 \sim Y_1$ and $X_2 \sim Y_2$ where t is an X_2 and a Y_1 variable. Then $(X_1 \vee X_2) \ni (t) \sim (Y_1 \vee Y_2) \ominus (t)$.*

Proof. Using the proof of Theorem 3,

$$X_1 \vee X_2 = (Y_1 \vee Y_2)\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}.$$

Take the equation for t and substitute for t into each other occurrence for t in this system of equations. Thus, we obtain $(X_1 \vee X_2) \ominus (t)$ as linear integer combination of $(Y_1 \vee Y_2) \ominus (t)$. To complete the proof, reverse the roles of $X_1 \vee X_2$ and $Y_1 \vee Y_2$.

In Jacobi's paper he solves the equation

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = fu$$

where f is the greatest common divisor of $\alpha_1, \alpha_2, \cdots, \alpha_n$. (That is, $f = (\alpha_1, \alpha_2, \cdots, \alpha_n)$.) He sets

$$u = y_1 = \left(\frac{\alpha_1}{f}\right)x_1 + \left(\frac{\alpha_2}{f}\right)x_2 + \cdots + \left(\frac{\alpha_n}{f}\right)x_n$$

and introduces certain variables $y_2, y_3, \cdots, y_n$ so that $X \sim Y$. Then the problem is solved since $X = YA$ and, with y_1 fixed, we can let $y_2, y_3, \cdots, y_n$ vary over all possible integer values and obtain all possible values of $X = (x_1, x_2, \cdots, x_n)$.

3. Two variable linear diophantine equations. In this section we give the usual Euclidean algorithm solution of

$$\alpha_1 x_1 + \alpha_2 x_2 = fu, \tag{1}$$

where α_1, α_2 are fixed integers and $f = (\alpha_1, \alpha_2)$. Of course $(\alpha_1/f, \alpha_2/f) = 1$ and

Euclid's algorithm provides us with integers γ and β such that

$$\gamma\frac{\alpha_1}{f}-\beta\frac{\alpha_2}{f}=1.$$

Then, if z is an arbitrary integer,

$$\alpha_1\left(\gamma u-\frac{\alpha_2}{f}z\right)+\alpha_2\left(-\beta u+\frac{\alpha_1}{f}z\right)=fu.$$

Our solution to (1) is then

$$x_1=\gamma u-\frac{\alpha_2}{f}z,\qquad x_2=-\beta u+\frac{\alpha_1}{f}z, \tag{2}$$

where z is an arbitrary integer.

To see that (2) has all (x_1,x_2) such that (1) holds, write (2) as

$$(x_1,x_2)=(u,z)\begin{bmatrix}\gamma & -\beta\\ \dfrac{-\alpha_2}{f} & \dfrac{\alpha_1}{f}\end{bmatrix}=(u,z)A.$$

Note that $\det A=1$. Thus $(x_1,x_2)\sim(u,z)$ and our solution is complete.

4. General linear diophantine equations. As we remarked in the first section, we wish to solve

$$\alpha_1x_1+\alpha_2x_2+\cdots+\alpha_nx_n=fu \tag{3}$$

where $f=(\alpha_1,\alpha_2,\cdots,\alpha_n)$ and $\alpha_1,\alpha_2,\cdots,\alpha_n$ are integer constants. The main task is to find $Y=(y_1,y_2,\cdots,y_n)$ such that $X\sim Y$. To do this some new equations must be introduced.

Let $f_2=(\alpha_1,\alpha_2)$. Then consider

$$\alpha_1x_1+\alpha_2x_2=f_2y_2.$$

By section 3, there exists z_1 such that $(x_1,x_2)\sim(z_1,y_2)$. Then let $f_3=(f_2,\alpha_3)$ and consider

$$f_2y_2+\alpha_3x_3=f_3y_3.$$

Again there exists z_2 such that $(y_2,x_3)\sim(z_2,y_3)$.

Letting $f_i=(f_{i-1},\alpha_i)$, $i=3,\cdots,n$, we obtain the following equations:

$$\begin{aligned}\alpha_1x_1+\alpha_2x_2&=f_2y_2,\\ f_2y_2+\alpha_3x_3&=f_3y_3,\\ f_3y_3+\alpha_4x_4&=f_4y_4,\\ &\cdots\cdots\\ f_{n-1}y_{n-1}+\alpha_nx_n&=f_ny_n.\end{aligned} \tag{4}$$

Of course $y_n = u$ and $f_n = f$.

Repeated applications of section 3 yield

$$
\begin{aligned}
&(x_1, x_2) \sim (z_1, y_2),\\
&(y_2, y_3) \sim (z_2, y_3),\\
&(y_3, x_4) \sim (z_3, y_4),\\
&\cdots\cdots\cdots\cdots\\
&(y_{n-1}, x_n) \sim (z_{n-1}, y_n).
\end{aligned}
\tag{5}
$$

Theorem 4 applied to the first two lines of (5) yields $(x_1, x_2, x_3) \sim (z_1, z_2, y_3)$ This relation and the third line (5) yields $(x_1, x_2, x_3, x_4) \sim (z_1, z_2, z_3, y_4)$. Proceeding in the same manner, we obtain

$$(x_1, x_2, \cdots, x_n) \sim (z_1, z_2, \cdots, z_{n-1}, y_n)$$

or

$$(x_1, x_2, \cdots, x_n) \sim (z_1, z_2, \cdots, z_{n-1}, u). \tag{6}$$

Of course our solution is obtained in the obvious way from (5). From the first two sets of equations, we eliminate y_2. Then successively, eliminate $y_3, y_4, \cdots, y_{n-1}$. This process was indicated in our passage from (5) to (6). Jacobi actually finds the matrices associated with (6) and therefore solves the linear diophantine equation. He shows the determinant of the two associated matrices is 1 but we do not include his further results here.

This work was partly performed under the auspices of the U. S. Atomic Energy Commission while the author was a faculty participant of the Associated Western Universities at Los Alamos Scientific Laboratory.

References

1. C. G. J. Jacobi, Über die Auflösung der Gleichung $\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n = fu$, J. Reine Angew. Math., 69 (1869) 1–28.

2. Ivan Niven and H. S. Zuckerman, An Introduction to the Theory of Numbers, Wiley, New York, London, 1960.