Linear Diophantine Equations

William J. Gilbert
University of Waterloo
Waterloo, Ontario
Canada N2L 3G1

Anu Pathria
University of California at Berkeley
Berkeley, CA 94720

AMS Classifications: Primary: 11D04; Secondary: 11A05, 15A36, 90C10

1990

If students can solve a system of linear equations by row reduction, we show how they can also find all the integer solutions to a system of linear Diophantine equations, using "integer" row reduction. When this method is applied to solve a single linear Diophantine equation in two variables, it reduces to the Euclidean Algorithm.

The Euclidean Algorithm

Equations with integer variables and integer coefficients are usually called *Diophantine equations*, after the Greek mathematician Diophantus of Alexandria, who wrote a famous treatise on arithmetic in the third century A. D.

The simplest non-trivial linear Diophantine equation is one with two variables of the form $ax + by = c$. This is usually solved by the Euclidean Algorithm. We will write the Euclidean Algorithm in terms of row reduction in such a way that the method will generalize to solve any linear system in any number of variables. Since we require integer solutions, the row reductions must only involve integers; this type of row operation is called unimodular. An *elementary unimodular row operation* on a matrix consists one of the following three types of operations.

(i) Add an integer multiple of one row of the matrix to another row.

(ii) Interchange two rows of the matrix.

(iii) Multiply one row of the matrix by -1.

EXTENDED EUCLIDEAN ALGORITHM. *Given any integers a and b, it is possible to unimodular row reduce* $\left[\begin{array}{c|cc} a & 1 & 0 \\ b & 0 & 1 \end{array}\right]$ *to* $\left[\begin{array}{c|cc} d & s & t \\ 0 & s_1 & t_1 \end{array}\right]$. *Then* $\gcd(a,b) = \pm d$ *and the general solution to the Diophantine equation* $ax + by = d$ *is*

$$\begin{aligned} x &= s + ks_1 \\ y &= t + kt_1 \end{aligned} \qquad \text{for } k \in \mathbb{Z}.$$

The formal proof of the Extended Euclidean Algorithm will follow from the general results we prove later. The validity of this algorithm can be motivated by noting that the row reduction implies that

$$\begin{bmatrix} s & t \\ s_1 & t_1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} d \\ 0 \end{bmatrix}.$$

Hence, for any integer k,

$$(s + ks_1)a + (t + kt_1)b = d$$

and $x = s + ks_1$, $y = t + kt_1$ certainly satisfies the equation $ax + by = d$.

Note that [4] also describes the traditional back-substitution to find x and y, in the Extended Euclidean Algorithm, in terms of row reduction.

EXAMPLE 1. *Solve the Diophantine equation* $91x + 21y = 7$.

Solution. Using unimodular row reduction

$$\left[\begin{array}{c|cc} 91 & 1 & 0 \\ 21 & 0 & 1 \end{array}\right] \longrightarrow \left[\begin{array}{c|cc} 7 & 1 & -4 \\ 21 & 0 & 1 \end{array}\right] \longrightarrow \left[\begin{array}{c|cc} 7 & 1 & -4 \\ 0 & -3 & 13 \end{array}\right].$$

Hence the general solution is $x = 1 - 3k$, $y = -4 + 13k$, for $k \in \mathbb{Z}$. □

In this example, $\gcd(91, 21)$ is 7. The more general Diophantine equation

$$91x + 21y = c$$

will have a solution if and only if c is divisible by 7 and, if $c = 7c'$, the solution is

$$x = c' - 3k, \quad y = -4c' + 13k \quad \text{for } k \in \mathbb{Z}.$$

This Extended Euclidean Algorithm can easily be entered on a programmable calculator that performs vector calculations.

Greatest Common Divisor

The greatest common divisor of any number of integers, $a_1, a_2, \ldots, a_m$, can be found using the following algorithm.

PROPOSITION. *It is always possible to unimodular row reduce the column matrix* $\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{bmatrix}$ *to* $\begin{bmatrix} d \\ 0 \\ \vdots \\ 0 \end{bmatrix}$, *where* $d = \gcd(a_1, a_2, \ldots, a_m)$.

Proof. Repeat the following process until there is only one non-zero entry.

(i) Let a_j be an element of $a_1, a_2, \ldots, a_m$ that has the smallest non-zero absolute value.

(ii) For each $i \neq j$, apply the Division Algorithm to obtain

$$a_i = k_i a_j + r_i \qquad \text{where } 0 \leq |r_i| < |a_j|.$$

(iii) For each $i \neq j$, subtract k_i times row j from row i.

Each time this process is applied, the largest absolute value of all the entries strictly decreases, unless all the non-zero entries have the same absolute value. In this exceptional case, all the entries, except one, become non-zero. Hence the algorithm terminates and, by interchanging rows and possibly multiplying one row by -1, we can move the non-zero entry to the top and make it positive.

Using any of the usual definitions of the greatest common divisor, it is easy to show that

$$\gcd(a_1, a_2, \ldots, a_m) = \gcd(a_1 - k_1 a_j, a_2, \ldots, a_m).$$

Hence

$$\begin{aligned} \gcd(a_1, a_2, \ldots, a_m) &= \gcd(a_1 - k_1 a_j, a_2 - k_2 a_j, \ldots, a_j, \ldots, a_m - k_m a_j) \\ &\vdots \\ &= \gcd(0, 0, \ldots, \pm d, \ldots, 0) \\ &= d. \end{aligned}$$

□

Systems of Linear Diophantine Equations

A general system of linear Diophantine equations can be written in matrix form as $AX = B$. We shall show how to determine whether this system has an integer solution and, if it does, how to find all its solutions. We shall need to use a weak definition of row-echelon form in which the leading entries (or pivots) are allowed be any integer and are not required necessarily to be 1. A matrix is said to be in *row-echelon form* if

(i) All the zero rows are at the bottom of the matrix.

(ii) The leading entry in each non-zero row is to the right of all the leading entries in the rows above it.

THEOREM. *To solve the system of linear Diophantine equations $AX = B$, unimodular row reduce $[A^t|I]$ to $[R|T]$, where R is in row-echelon form. Then the system $AX = B$ has integer solutions if and only if the system $R^tK = B$ has integer solutions for K, and all the solutions of $AX = B$ are of the form $X = T^tK$.*

The matrix equation $R^tK = B$ can be easily solved for K by back-substitution. A typical equation looks like

$$\begin{bmatrix} d_1 & & & \\ * & d_2 & & \\ * & * & & \\ * & * & d_3 & \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix} \begin{bmatrix} k_1 \\ k_2 \\ k_3 \\ \vdots \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ \vdots \end{bmatrix}.$$

Proof. The previous proposition shows how to unimodular row reduce the matrix A^t into row-echelon form. First row reduce A^t so that its first column begins with the greatest common divisor and has all zeros below. Then leave the first row alone and row reduce the other rows so as to maneuver the second column to the required form. Continue in this manner.

The row reduction of $[A^t|I]$ to $[R|T]$ corresponds to premultiplication by an invertible matrix E; that is

$$E[A^t|I] = [R|T].$$

Hence $T = E$, which is invertible, and $TA^t = R$. Therefore $AT^t = R^t$ and $A = R^t(T^t)^{-1}$.

Now the matrix T is a product of elementary matrices corresponding to the unimodular row operations that were performed. Each of these elementary matrices has determinant ± 1 so $\det T = \pm 1$. Hence

$$(T^t)^{-1} = \operatorname{adj}(T^t)/\det T^t = \pm \operatorname{adj}(T^t)$$

and has all its entries integers.

The equation $AX = B$ is equivalent to $R^t(T^t)^{-1}X = B$. Write $K = (T^t)^{-1}X$, so $X = T^tK$ and X has integer entries if and only if K does. The system $AX = B$ now has integer solutions for X if and only if the system $R^tK = B$ has integer solutions for K. □

EXAMPLE 2. *Find all the integer solutions to the following system of equations.*

$$\begin{aligned} 5x_1 + 6x_2 + 8x_3 &= 1 \\ 6x_1 - 11x_2 + 7x_3 &= 9 \end{aligned}$$

Solution. Using unimodular row reduction

$$\left[\begin{array}{rr|ccc} 5 & 6 & 1 & 0 & 0 \\ 6 & -11 & 0 & 1 & 0 \\ 8 & 7 & 0 & 0 & 1 \end{array}\right] \longrightarrow \left[\begin{array}{rr|ccc} 5 & 6 & 1 & 0 & 0 \\ 1 & -17 & -1 & 1 & 0 \\ 3 & 1 & -1 & 0 & 1 \end{array}\right] \longrightarrow \left[\begin{array}{rr|ccc} 1 & -17 & -1 & 1 & 0 \\ 0 & 91 & 6 & -5 & 0 \\ 0 & 52 & 2 & -3 & 1 \end{array}\right]$$

$$\longrightarrow \left[\begin{array}{rr|ccc} 1 & -17 & -1 & 1 & 0 \\ 0 & -13 & 2 & 1 & -2 \\ 0 & 52 & 2 & -3 & 1 \end{array}\right] \longrightarrow \left[\begin{array}{rr|ccc} 1 & -17 & -1 & 1 & 0 \\ 0 & 13 & -2 & -1 & 2 \\ 0 & 0 & 10 & 1 & -7 \end{array}\right].$$

The equation $R^tK = B$ is

$$\begin{bmatrix} 1 & 0 & 0 \\ -17 & 13 & 0 \end{bmatrix} \begin{bmatrix} k_1 \\ k_2 \\ k_3 \end{bmatrix} = \begin{bmatrix} 1 \\ 9 \end{bmatrix};$$

hence $k_1 = 1$ and $-17k_1 + 13k_2 = 9$. Therefore $13k_2 = 26$ and, since the right side is divisible by 13, the equation has an integer solution, namely $k_2 = 2$. The variable k_3 can be any integer value, say $k_3 = k \in \mathbb{Z}$. Therefore

$$K = \begin{bmatrix} 1 \\ 2 \\ k \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = T^tK = \begin{bmatrix} -1 & -2 & 10 \\ 1 & -1 & 1 \\ 0 & 2 & -7 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ k \end{bmatrix} = \begin{bmatrix} -5 + 10k \\ -1 + k \\ 4 - 7k \end{bmatrix}.$$

The complete integer solution is therefore

$$\begin{aligned} x_1 &= -5 + 10k \\ x_2 &= -1 + k \qquad \text{for } k \in \mathbb{Z}. \\ x_3 &= 4 - 7k \end{aligned}$$

□

EXERCISE. *Find all the integer solutions to* $6x_1 - 14x_2 + 21x_3 = 11$.

In general, the question of whether the system has any integer solutions at all depends on whether certain combinations of the right side are zero or are divisible by the pivots of R. In Example 2 above, the pivots (leading entries) are 1 and 13. If the entries on the right side were b_1 and b_2, the system would have a solution if and only if the equations $k_1 = b_1$ and $-17k_1 + 13k_2 = b_2$ would have integer solutions. This would happen if and only if $17b_1 + b_2$ were divisible by 13.

In solving a large system, you can check each row of the system $R^tK = B$ as you go along to determine whether the system still has a solution. If there is no solution, you might not have to complete the row reduction.

Further Reading

You might expect the solution to a system of linear Diophantine equations to be part of a subject called "Integer Linear Algebra." However there is no such subject; it is a part of Integer Linear Programming. In order to find all integer solutions to the equation

$$a_1x_1 + \cdots + a_nx_n = b$$

we essentially have to determine $\gcd(a_1, \ldots, a_n)$, which is the minimum positive value of the left side of the equation as the variables run over all the integers; this is a Linear Programming problem. Hence you will find further information on systems of linear equations and congruences in books on Integer Programming such as [2, Ch.6] and [3, Chs. 4 and 5].

We have expressed the algorithm in terms of row reductions, since students are accustomed to these operations. However, it is more natural to use *column operations* on the matrix $\begin{bmatrix} A \\ \hline I \end{bmatrix}$. If A is of full row rank then A

can be unimodular column reduced to its *Hermite normal form.* This is the column-echelon form in which all entries are non-negative and each pivot is the maximum entry in its row [3, §4.1]. Therefore the algorithm in the theorem of this paper essentially involves the reduction of A to its Hermite normal form.

An issue that we have not addressed, but which becomes vital when solving a large system on a computer, is the efficiency of the algorithm. While the algorithm only performs a polynomial number of row operations, relative to the size of the input, it appears that the matrix *entries* grow exponentially with the size of the system. Polynomial time algorithms for reducing an integer matrix to its Hermite normal form are given in [3, §5.3] and [1]. These techniques can be translated into polynomial running time algorithms to solve a system of linear Diophantine equations.

References

[1] P. D. Domich, R. Kannan and L. E. Trotter, Hermite Normal Form Computation using Modulo Determinant Arithmetic, *Mathematics of Operations Research* 12 (1987), 50–59.

[2] H. Greenberg, *Integer Programming*, Academic Press, New York, 1971.

[3] A. Schrijver, *Theory of Linear and Integer Programming*, Wiley, Chichester, 1986.

[4] K.-W. Yang, Euclid's Algorithm = Reverse Gaussian Elimination, *Math. Mag.* 63 (1990), 163–164.