5 Linear Equations

Basic problem: Fix $a_1, \ldots, a_n \in \mathbb{Z},\ n > 0$. Consider the equation:

$$a_1x_1 + \ldots a_nx_n = \vec{a} \cdot \vec{x} = m, \tag{*}$$

where $\vec{a} = (a_1, \ldots, a_n)$ and $\vec{x} = (x_1, \ldots, x_n)$. Determine if (*) can be solved **in integers**. If so, determine all the solutions.

These are the simplest Diophantine Equations.

Earlier, we proved that, given $a_1, \ldots, a_n \in \mathbb{Z}$, not all zero, $\exists!$ positive integer d, the **greatest common devisor**, such that we can solve

$$a_1x_1 + \ldots a_nx_n = m$$

if m is a multiple of d, and that the set

$$M = \{a_1x_1 + \ldots a_nx_n > 0 | x_1, \ldots, x_n \in \mathbb{Z}\}$$

is simply $d\mathbb{Z}$. Moreover, d is the smallest number in $M^+ = \{r \in M | r > 0\}$, which exists by the WOA.

Consequently we have

Lemma 1. (*) can be solved iff m is a multiple of gcd $(\{a_i\})$.

So the basic problem comes down to determining all solutions of $a \cdot x = dN$, for any $N \geq 1$.

Suppose **n=1**; then it is trivial. We have:

$$a_1 \neq 0,\ d = gcd = |a_1|,$$

and we need to solve

$$a_1x_1 = |a_1|N \tag{$*_N$}$$

But there is a **unique** solution, namely:

$$x_1 = sgn(a_1)N$$

n=2:

First look at case **gcd=1**, **N=1**.

$$a_1x_1 + a_2x_2 = 1 \tag{$*_1$}$$

By Lemma 1 there exists a solution, call it (u_1, u_2). Suppose (v_1, v_2) is another solution. Then

$$a_1 u_1 + a_2 u_2 = 1 \tag{1}$$

$$a_1 v_1 + a_2 v_2 = 1 \tag{2}$$

Multiply (1) by v_1; (2) by u_1:

$$\begin{aligned}
&a_1 u_1 v_1 + a_2 u_2 v_1 = v_1 \\
&\underline{a_1 u_1 v_1 + a_2 u_1 v_2 = u_1} \\
&a_2(v_1 u_2 - u_1 v_2) = v_1 - u_1 = k
\end{aligned}$$

Do same with (1) times v_2, (2) times u_2 to get:

$$a_1 \underbrace{(u_1 v_2 - u_2 v_1)}_{-k} = (v_2 - u_2)$$

So

$$v_1 = u_1 + k a_2, \quad v_2 = u_2 - k a_1.$$

(u_1, u_2) is a **particular solution** which we use to generate all solutions.

Conversely, for **any** integer k,

$$(u_1 + k a_2,\ u_2 - k a_1)$$

is a solution of $\vec{a} \cdot \vec{x} = 1$.

If gcd $(a_1, a_2) = 1$, then we can solve $a_1 x_1 + a_2 x_2 = 1$ in integers. Moreover, if (u_1, u_2) is a particular solution, then any other solution is of the form $(u_1 + k a_2, u_2 - k a_1),\ k \in \mathbb{Z}$.

n=2, **d** $>$**1**, **N=1**:

$$a_1 x_1 + a_2 x_2 = d \tag{$*_1$}$$

Since $d =$gcd(a_1, a_2), $d | a_1$ and $d | a_2$. Put $b_i = \frac{a_i}{d}$. Then (*) becomes

$$b_1 x_1 + b_2 x_2 = 1 \text{ with } (b_1, b_2) = 1.$$

So if (u_1, u_2) is a particular solution, every solution is of the form

$$\left(u_1 + k\frac{a_2}{d},\ u_2 - k\frac{a_1}{d}\right).$$

This finishes the $n = 2$ case. We summarize the results in the following

Proposition *Let a_1, a_2 be non-zero integers, and let d be their gcd. Then the equation*

$$a_1x_1 + a_2x_2 = m$$

is solvable in integers iff m is divisible by d. Moreover, if (u_1, u_2) is any particular solution, then the set of all solutions is parametrized by $\mathbb{Z}$, and for each $r \in \mathbb{Z}$, the corresponding solution is given by

$$x_1 = u_1 + r\frac{a_2}{d}, \quad \text{and} \quad x_2 = u_2 - r\frac{a_1}{d}.$$

$\mathbf{n}, \mathbf{a}, \mathbf{N}$ arbitrary: (general case)

It will be good to understand the example at the end of the section (for $n = 3$). The rest of the section may be difficult and is included here for completeness.

Definition:

$$M_n(\mathbb{Z}) = \{a = (a_{ij}) : \ n \times n - \text{matrices with } a_{ij} \in \mathbb{Z}\ \forall i, j\}.$$

$$I_n = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}$$

$$GL_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) : \det(A) = \pm 1\}$$

The equation of interest is

$$(a_1, \dots, a_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = Nd \qquad (*_N)$$

Lemma 1 *Let $a = (a_1, \cdots, a_n) \in \mathbb{Z}^n - \{0\}$ with $d = \gcd(a_1, \cdots, a_n)$. Then $\exists\, C \in GL_n(\mathbb{Z})$ such that $aC = de_n = (0, \cdots, 0, d)$.*

Proof. $n = 1$: $\quad d = |a_1|$, so we can take $C = (sgn(a_1))$. Now let $n > 1$, and assume Lemma by induction for $m < n$. If $a_1 = \cdots = a_{n-1} = 0$ we can take

$$C = \left(\begin{array}{c|c} I & 0 \\ \hline 0 & \text{sgn } (a_n) \end{array} \right).$$

So we may suppose that $a' := (a_1, \cdots, a_{n-1}) \in \mathbb{Z}^{n-1} - \{0\}$.

Let $d' = \gcd(a_1, \cdots, a_{n-1})$. By the inductive hypothesis, $\exists\, C' \in GL_{n-1}(\mathbb{Z})$ such that $a'\, C' = (0, \cdots, d') \in \mathbb{Z}^{n-1}$.

Let

$$A = \left(\begin{array}{c|c} C' & 0 \\ \hline 0 & 1 \end{array} \right) \in GL_n\,(\mathbb{Z}).$$

Then $aA = (0, \cdots, 0, d', a_n)$. Clearly, $d = \gcd(d', a_n)$, and $\exists\, x, y \in \mathbb{Z}$ such that $d'x + a_n\, y = d$.

Put

$$B = \begin{pmatrix} a_n/d & x \\ -d'/d & y \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Then $(d', a_n)\, B = (0, d)$.

Put

$$C = A \left(\begin{array}{c|c} I_{n-2} & 0 \\ \hline 0 & B \end{array} \right) \in GL_n\,(\mathbb{Z}).$$

Then

$$\begin{aligned} aC = (aA) \left(\begin{array}{c|c} I_{n-2} & 0 \\ \hline 0 & B \end{array} \right) &= (0, \cdots, 0, d', a_n) \left(\begin{array}{c|c} I_{n-2} & 0 \\ \hline 0 & B \end{array} \right) &\quad (3) \\ &= (0, \cdots, 0, d). &\quad (4) \end{aligned}$$

Theorem 5.1 *Let $a = (a_1, \cdots, a_n) \in \mathbb{Z}^n - \{0\}$ with* gcd *equal to d.*

Let C be the matrix given by Lemma. Pick any $N \in \mathbb{Z}$. Then we have:

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{Z}^n$$

is a solution of $\sum_{i=1}^{n} a_i\, x_i = Nd$ if and only if $\exists m_1, \cdots, m_{n-1} \in \mathbb{Z}$ such that

$$x = \sum_{i=1}^{n-1} m_i C^i + N C^n$$

where C^j denotes $(\forall j)$ the j-th column of C.

Proof.

Let $y = x - NC^n$.

Then

$$a \cdot x = Nd \Leftrightarrow a{\cdot}y = 0$$
$$\Updownarrow$$
$$aC(C^{-1}y) = (0, \cdots, 0, d)(C^{-1}y) = 0$$
$$\Updownarrow$$
$$C^{-1}y = m = \begin{pmatrix} m_1 \\ 1 \\ 1 \\ m_{n-1} \\ 0 \end{pmatrix}, \text{ for some } m_i \in \mathbb{Z}, 1 \le i \le n-1$$
$$\Updownarrow$$
$$y = Cm = \sum_{i=1}^{n-1} m_i C^i$$
$$\Updownarrow$$
$$x = Cm + NC_n.$$

Example: Find all the integral solutions of

$$5x + 7y + 11z = 2. \qquad (*)$$

Put $a = (5,\, 7,\, 11)$. Then the gcd of the coordinates of a is 1. By Lemma, we can find a 3×3 - integral matrix C of determinant ± 1 such that $aC = (0,\, 0,\, 1)$. The proof of Lemma gives a recipe for finding C. First solve $5x + 7y = 1$. Since $1 = \gcd(5,\, 7)$, this can be solved, and a solution (by inspection) is given by $x = -4$, $y = 3$. Put $C' = \begin{pmatrix} 7 & -4 \\ -5 & 3 \end{pmatrix}$. Next we have to solve $d'u + 11v = 1$, where $d' = \gcd(a_1, a_2) = 1$. A solution is given by $u = 1$, $v = 0$. Let $B = \begin{pmatrix} 11 & 1 \\ -1 & 0 \end{pmatrix}$.

Then the proof of Lemma says that

$$C = \left(\begin{array}{cc|c} \multicolumn{2}{c|}{\multirow{2}{*}{C'}} & 0 \\ & & 0 \\ \hline 0 & 0 & 1 \end{array} \right) \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & \multicolumn{2}{c}{\multirow{2}{*}{B}} \\ 0 & & \end{array} \right).$$

Matrix multiplication gives

$$C = \begin{pmatrix} 7 & -44 & -4 \\ -5 & 33 & 3 \\ 0 & -1 & 0 \end{pmatrix}.$$

By the Theorem, the complete set of integral solutions of (*) is given by:

$$\begin{bmatrix} x = 7m - 44n - 8 \\ y = -5m + 33n + 6 \\ z = -n \end{bmatrix} \quad \text{where } m,\, n \in \mathbb{Z}$$