Chapter 18 – Linear Diophantine Equations

A Diophantine equation is an equation involving integers for which one asks for integer solutions.

Problem: Given integers a, b, c, find all integers m and n s.t.

$$am + bn = c.$$

i.e. write c as an integer linear combination of a and b in all possible ways.

Observation: If $c = am + nb$ for some $m, n \in \mathbb{Z}$, then $\gcd(a,b)$ divides c (because $\gcd(a,b)$ divides a and divides b).

→ So $\gcd(a,b) \mid c$ is a necessary condition for the existence of an integer solution to the equation $am + bn = c$.

But clearly this is also a sufficient condition since $\exists\, m', n' \in \mathbb{Z}$ s.t. $\gcd(a,b) = am' + bn'$ so that if $c = q \cdot \gcd(a,b)$, $q \in \mathbb{Z}$, then

$$c = a(\underbrace{qm'}_{m}) + b(\underbrace{qn'}_{n}).$$

Thm. 17.1.1. →

As a direct consequence of Theorem 17.1.1 we therefore have:

Theorem 18.2.1: For $a, b, c \in \mathbb{Z}$,

$$\exists\, m, n \in \mathbb{Z} \text{ s.t. } am + bn = c \iff \gcd(a,b) \mid c.$$

So we know when solutions exist, but how do we find all solutions?

Before dealing with the general case we need to understand the homogeneous case, i.e. the case where $c = 0$.

The Homogeneous Case:

Problem: Given $a, b \in \mathbb{Z}$, find all integer solutions to the equation

$$am + bn = 0. \tag{1}$$

Step 1: Simplify. Find $\gcd(a,b)$ and divide the equation by $\gcd(a,b)$ to get

$$\hat{a}m + \hat{b}n = 0 \tag{2}$$

where $\hat{a} = \frac{a}{\gcd(a,b)}$ and $\hat{b} = \frac{b}{\gcd(a,b)}$.

note $\gcd(\hat{a}, \hat{b}) = 1$

Step 2: Solve equation (2):

Equations (1) and (2) have the same solutions. The solutions are given by the following proposition.

Proposition: Let $\hat{a}, \hat{b} \in \mathbb{Z}$ with $\gcd(\hat{a}, \hat{b}) = 1$. Then, for $m, n \in \mathbb{Z}$,

$$\hat{a}m + \hat{b}n = 0 \iff (m,n) = (\hat{b}q, -\hat{a}q) \text{ for some } q \in \mathbb{Z}.$$

↳ i.e. $m = \hat{b}q$ and $n = -\hat{a}q$

Proof: Let $m, n \in \mathbb{Z}$.

The reverse implication is clear: If $m = \hat{b}q$ and $n = -\hat{a}q$ for some $q \in \mathbb{Z}$ then

$$\hat{a}m + \hat{b}n = \hat{a}\hat{b}q - \hat{b}\hat{a}q = 0.$$

Forward implication: Suppose $\hat{a}m + \hat{b}n = 0$. Then $\hat{a}m = -\hat{b}n = \hat{b}(-n)$, so $\hat{b} \mid \hat{a}m$.

By the theorem from page 6 of the notes on Ch. 17 →

But $\gcd(\hat{a}, \hat{b}) = 1$, so $\hat{b} \mid m$. Hence $\exists q \in \mathbb{Z}$ s.t. $m = \hat{b}q$. But then $\hat{a}(\hat{b}q) + \hat{b}n = 0$, so $n = -\hat{a}q$.

This proves the result. □

So the general solution to (1) is given by $(m,n) = (\hat{b}q, -\hat{a}q)$ where $q \in \mathbb{Z}$.

The General Case

We now consider the case where $c \neq 0$.

Problem: Given integers a, b, c, with $c \neq 0$, find all integer solutions of the equation

$$am + bn = c. \tag{1}$$

Step 1: Find $\gcd(a,b)$.

- If $\gcd(a,b)$ does not divide c, then there are no solutions!
- If $\gcd(a,b) \mid c$, then divide both sides of the equation by $\gcd(a,b)$ to get

$$\hat{a}m + \hat{b}n = \hat{c} \tag{2}$$

where $\hat{a} = \frac{a}{\gcd(a,b)}$, $\hat{b} = \frac{b}{\gcd(a,b)}$, and $\hat{c} = \frac{c}{\gcd(a,b)}$.

note $\gcd(\hat{a},\hat{b}) = 1$

Step 2: Find one solution of equation (2).

Equations (1) and (2) have the same solutions. To find a particular solution of (2) we first use the Euclidean Algorithm, followed by back substitution, to

find a particular solution to the equation

(3) $\hat{a}m' + \hat{b}n' = 1$, ← $\gcd(\hat{a},\hat{b}) = 1$

$m', n' \in \mathbb{Z}$. Then $m = \hat{c}m'$ and $n = \hat{c}n'$ solve (2). ← Hence they also solve (1).

Remark: It is a good idea to call the particular solution (m,n) we find in this step (m_1, n_1). (i.e. $m_1 = \hat{c}m'$, $n_1 = \hat{c}n'$)

Step 3: To go from having one solution to having all solutions, one now only has to solve the corresponding homogeneous equation. This is because of the following simple observation:

Proposition: Let $a, b, c \in \mathbb{Z}$ and suppose $m_1, n_1 \in \mathbb{Z}$ satisfy $am_1 + bn_1 = c$. Then $m_2, n_2 \in \mathbb{Z}$ satisfy $am_2 + bn_2 = c$ if and only if $m_2 = m_1 + m_0$ and $n_2 = n_1 + n_0$ where $m_0, n_0 \in \mathbb{Z}$ satisfy

$$am_0 + bn_0 = 0.$$

↕ equivalently $\hat{a}m_0 + \hat{b}n_0 = 0$ where $\hat{a} = \frac{a}{\gcd(a,b)}$ and $\hat{b} = \frac{b}{\gcd(a,b)}$.

The general solution to the homogeneous equation $\hat{a}m_0 + \hat{b}n_0 = 0$ is

$$(m_0, n_0) = (\hat{b}q, -\hat{a}q), \quad q \in \mathbb{Z}.$$

$\longrightarrow$ General solution to $am + bn = c$:

Let (m_1, n_1) denote the particular solution to (1) found in Step 2. The general solution to (1) is

$$(m, n) = (m_1 + \hat{b}q, n_1 - \hat{a}q), \text{ where } q \in \mathbb{Z}.$$

$\uparrow$ i.e. $(m, n) = (m_1 + m_0, n_1 + n_0)$ where (m_0, n_0) is a solution of the corresponding homogeneous equation.

Let's see some examples of this general procedure.

Examples:

- Find all integer solutions to

$$140m + 63n = 10.$$

Solution: We start by finding $\gcd(140, 63)$, using the Euclidean Algorithm:

$$140 = 63 \times 2 + 14$$
$$63 = 14 \times 4 + \boxed{7}$$
$$14 = 7 \times 2 + 0.$$

Since $\gcd(140, 63) = 7$ does not divide 10, there are no solutions.

- Find all integer solutions to

$$\underbrace{140}_{a}m + \underbrace{63}_{b}n = \underbrace{35}_{c}.$$

Solution:

Step 1: Note that $\gcd(140, 63) = 7$ divides 35. We divide by 7 to obtain the equivalent equation

$$\underbrace{20}_{\hat{a}}m + \underbrace{9}_{\hat{b}}n = \underbrace{5}_{\hat{c}}.$$

Step 2: We solve $20m' + 9n' = 1$.

↑ really we just find one particular solution of this.

Euclidean Algorithm:

$$20 = 9 \times 2 + 2 \qquad 2 = 20 - 9 \times 2$$
$$9 = 2 \times 4 + \boxed{1} \qquad 1 = 9 - 2 \times 4$$
$$2 = 1 \times 2 + 0$$

$$1 = 9 - 2 \times 4$$
$$= 9 - (20 - 9 \times 2) \times 4$$
$$= 20 \times \underbrace{(-4)}_{m'} + 9 \times \underbrace{9}_{n'}$$

We get $m' = -4$ and $n' = 9$, and so

($m_1 = \hat{c}m'$, $n_1 = \hat{c}n'$) $m_1 = 5 \times (-4) = -20$ and $n_1 = 5 \times 9 = 45$ satisfy $20m_1 + 9n_1 = 5$, and hence $140m_1 + 63n_1 = 35$.

Step 3: Hence the general solution to the Diophantine equation $140m + 63n = 35$ is given by

$$(m, n) = (\underbrace{-20}_{m_1} + \overset{+}{\downarrow}\underbrace{9}_{\hat{b}}q, \underbrace{45}_{n_1} - \overset{-}{\downarrow}\underbrace{20}_{\hat{a}}q)$$

where $q \in \mathbb{Z}$.