Lecture 9: The Diophantine equation 1

The simplest Diophantine equation is

$$ax+by=c \qquad a,b,c\in\mathbb{Z},\ a,b \text{ not both zero.}$$

A solution of this equation is a pair of integers x_0, y_0 which when substituted in the equation satisfy it. A Diophantine equation can have more than one solution, unique solution or no solution at all.

Theorem 9.1 The linear Diophantine equation $ax+by=c$ has a solution if and only if $d|c$, where $d=\gcd(a,b)$. If x_0, y_0 is any particular solution of this equation then all other solutions are given by:

$$x=x_0+\left(\frac{b}{d}\right)t \ , \ y=y_0-\left(\frac{a}{d}\right)t$$

where t is any arbitrary integer.

Proof Suppose the equation

$$ax+by=c \qquad -(I)$$

has a solution say (x_0, y_0). Hence

$$ax_0+by_0=c \qquad -(II)$$

Since $d=\gcd(a,b)$, therefore $d|a$ and $d|b$. Hence $\exists$ $r,s\in\mathbb{Z}$ such that

$$a=dr \text{ and } b=ds \qquad -(III)$$

(II) and (III) $\Rightarrow$ $c=drx_0+dsy_0=d(rx_0+sy_0)$

$\Rightarrow d|c$

Conversely suppose $d|c$. This gives us integer t such that $c=dt$.

Since $d=\gcd(a,b)$, $\exists\ x_0, y_0 \in \mathbb{Z}$ such that

$$d = ax_0 + by_0$$

$$\Rightarrow c = dt = (ax_0 + by_0)t = a(x_0 t) + b(y_0 t)$$

Hence $\exists$ solutions $(x_0 t, y_0 t)$ of the equation ①

Now we prove the second assertion. Suppose x_0, y_0 is a solution of the equation ①. Suppose x', y' is another solution of ①.
Then we have

$$ax_0 + by_0 = c = ax' + by'$$

$$\Rightarrow a(x' - x_0) = b(y_0 - y') \quad \text{---(V)}$$

Since $d=\gcd(a,b)$, hence $d|a$ and $d|b$ and hence $\exists$ relatively prime integers r and s such that

$$a = dr \text{ and } b = ds$$

Then we have

$$dr(x' - x_0) = ds(y_0 - y')$$

$$\Rightarrow r(x' - x_0) = s(y_0 - y') \quad \text{---(IV)}$$

$$\Rightarrow r \mid s(y_0 - y')$$

$$\Rightarrow r \mid (y_0 - y') \quad [\because \gcd(r,s) = 1 \text{ and Euclid's lemma}]$$

Hence $\exists\ t \in \mathbb{Z}$ such that

$$y_0 - y' = rt \quad \text{i.e.} \quad y' = y_0 - rt$$

Substituting the value of y' in (iv) gives us:

$$r(x' - x_0) = s(rt)$$

$$\Rightarrow x' = x_0 + st$$

Hence $x' = x_0 + \frac{b}{d}t$, $y' = y_0 - \frac{a}{d}t$

Example We will find the solution of the linear Diophantine equation.

$$172x + 20y = 1000$$

Solution First we find the gcd $(172, 20)$.

$$d = \gcd(172, 20) = 4$$

$$\begin{aligned} 172 &= 8 \cdot 20 + 12 \\ 20 &= 1 \cdot 12 + 8 \\ 12 &= 1 \cdot 8 + 4 \\ 8 &= 2 \cdot 4 \end{aligned}$$

} Euclidean algorithm

Since $4 \mid 1000$, therefore the given equation has solution

Next we write 4 as a linear combination of 172 and 20.

$$\begin{aligned} 4 &= 12 - 8 \\ &= 12 - (20 - 12) \\ &= 2 \cdot 12 - 20 \\ &= 2(172 - 8 \cdot 20) - 20 \end{aligned}$$

$$\Rightarrow 4 = 2 \cdot 172 + (-17)20$$

Multiplying this relation by 250 we get

$$1000 = 250 \cdot 4 = 250\,[2 \cdot 172 + (-17)20]$$

$$= 500 \cdot 172 + (-4250)20$$

Hence $x_0 = 500$ and $y_0 = -4250$ is a solution of the given eqn.

All other solutions are expressed as:

$$x = 500 + (20/4)t = 500 + 5t$$

$$y = -4250 - (172/4)t = -4250 - 43t \qquad t \in \mathbb{Z}$$

* Suppose we want solutions in positive integers. Then t must be chosen such that

$$5t + 500 > 0 \qquad -43t - 4250 > 0$$

i.e. $t > -10 \qquad -98\frac{36}{43} > t$.

i.e. $\quad -98\frac{36}{43} > t > -100$

$\Rightarrow t = -99$

Thus the given equation has unique positive solutions:

$$x = 500 + 5(-99) = 5$$

$$y = -4250 - 43(-99) = 7$$

Corollary 9.2. If $\gcd(a,b) = 1$ and if x_0, y_0 is a particular solution of the linear Diophantine equation $ax + by = c$ then all solutions are given by $x = x_0 + bt$, $y = y_0 - at$. $t \in \mathbb{Z}$