IV.18. Linear diophantine equations

**Theorem 1 (Eccles 18.2.1)** Let $a, b, c \in \mathbb{Z}^+$. Then there exist $m, n \in \mathbb{Z}$ such that

$$am + bn = c$$

if and only if $\gcd(a, b)$ divides $c$.

In other words,

**Equivalent Theorem** Given positive integers $a, b, c$ we can solve the equation $am + bn = c$ for some pair of integers $m, n$ if and only if $c$ is divisible by $\gcd(a, b)$.

**Proof.** ($\Leftarrow$) Suppose $\gcd(a, b)$ divides $c$. By Theorem 17.1.1, there exist $\bar{m}, \bar{n} \in \mathbb{Z}$ such that

$$\gcd(a, b) = a\bar{m} + b\bar{n}.$$ 

Since $\gcd(a, b)$ divides $c$, there exists $q \in \mathbb{Z}$ such that

$$c = \gcd(a, b) \cdot q.$$ 

Thus

$$c = \gcd(a, b) \cdot q = (a\bar{m} + b\bar{n}) q = a(\bar{m}q) + b(\bar{n}q).$$

Taking $m = \bar{m}q$ and $n = \bar{n}q$ yields $am + bn = c$.

($\Rightarrow$) Suppose there exist $m, n \in \mathbb{Z}$ such that $am + bn = c$. Since $\gcd(a, b)$ divides both $m$ and $n$, it divides $am + bn$. Now, since $am + bn = c$, we conclude that $\gcd(a, b)$ divides $c$. ■
So we know when the equation $am + bn = c$ has at least 1 solution. Now, when it has a solution, how do we describe all solutions?

**Example.** We have that $m_0 = 1$ and $n_0 = 2$ solve $60 = 24m_0 + 18n_0$, that is,

$$60 = 24 \cdot 1 + 18 \cdot 2.$$

We now describe all solutions. Suppose that $m$ and $n$ also solve

$$60 = 24m + 18n.$$

Then, taking the difference we get:

$$0 = 24m + 18n - (24 \cdot 1 + 18 \cdot 2) = 24 (m - 1) + 18 (n - 2).$$

This equation is equivalent to the one obtained by dividing by $\gcd (24, 18) = 6$, namely

$$-3 (n - 2) = 4 (m - 1).$$

Since $\gcd (3, 4) = 1$ and 3 divides $4 (m - 1)$, by Theorem 17.3.2 we conclude that 3 divides $m - 1$. Hence there exists an integer $k$ such that

$$m - 1 = 3k.$$

Thus

$$-3 (n - 2) = 4 (m - 1) = 4 \cdot 3k,$$

so that

$$n - 2 = -4k.$$

We have shown that if $m, n$ is any solution, then

$$m = 1 + 3k,$$

$$n = 2 - 4k,$$

where $k$ is an integer.

Conversely, $m = 1 + 3k$ and $n = 2 - 4k$ is indeed a solution for any integer $k$.

We have classified all solutions to the equation $60 = 24m + 18n$. 

2