3.7 Linear Diophantine Equations

How do you get \$510 in \$20 and \$50 bills?

We will need to solve the equation

$$20x + 50y = 510, \text{ or equivalently,}$$
$$2x + 5y = 51$$

for positive integer values of x and y.

By trial and error, we may find some integer solutions as shows below.

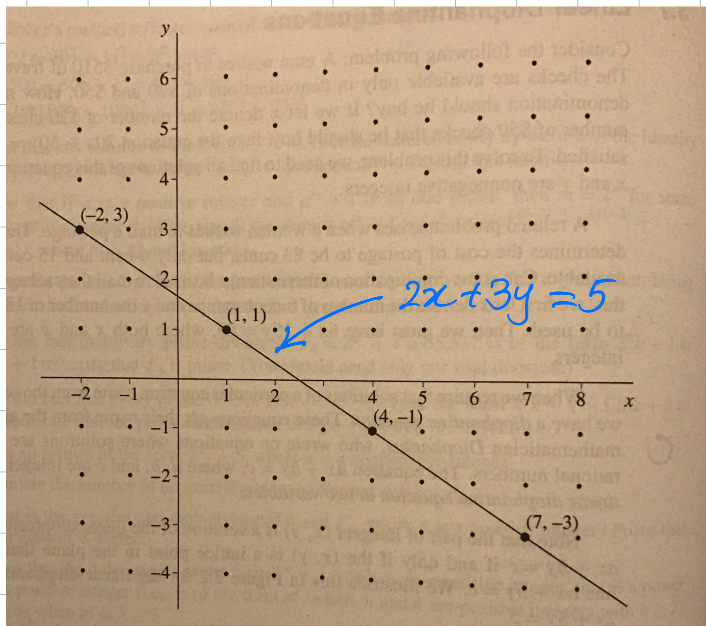
$x = 3, \quad y = 9$
$x = 8, \quad y = 7$
$x = 13, \quad y = 5$
$x = 18, \quad y = 3$
$x = 23, \quad y = 1$
$x = 28, \quad y = -1$

Definition: If we are interested in integer solutions of a particular equation, then that equation is called a diophantine equation. The equation

$$ax + by = c$$

where $a, b, c \in \mathbb{Z}$ is called a linear diophantine equation in two variables.

A graphical interpretation of the solutions of $2x+3y=5$ is given below.



Theorem 3.23: Consider the diophantine equation $ax+by=c$, where $a,b \in \mathbb{Z}$. Let $d = \gcd(a,b)$.

(i) If $d \nmid c$ then it has no solutions.

(ii) If $d \mid c$, then there are infinitely many solutions. Moreover, if $x = x_0$, $y = y_0$ is any solution, then all solutions are given by

$$x = x_0 + \left(\frac{b}{d}\right)n$$

$$y = y_0 - \left(\frac{a}{d}\right)n$$

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

Proof: (i) Suppose $d \nmid c$ and a solution $x = x_0$, $y = y_0$ exists.

Then, $ax_0 + by_0 = c$.

Since $d = \gcd(a,b)$, we've

$$d \mid (ax_0 + by_0).$$

$$\Rightarrow d \mid c, \text{ a contradiction.}$$

$\therefore$ if $d \nmid c$, no solution exists.

(ii) Assume $d \mid c$.

By Theorem 3.8, $\exists\ s,t \in \mathbb{Z}$ such that

$$d = sa + tb.$$

Since $d \mid c$, we've $c = de$ for some $e \in \mathbb{Z}$.

$$\therefore c = (sa + tb)e$$

$$\therefore c = a(se) + b(te)$$

$\therefore x = se$, $y = te$ is a solution.

To show that there are infinitely many solutions, consider, for each $n \in \mathbb{Z}$,

$$x_n = x_0 + \left(\frac{b}{d}\right)n \text{ and } y_n = y_0 - \left(\frac{a}{d}\right)n$$

where $x_0 = se$ and $y_0 = te$.

Then,

$$ax_n + by_n = a\left(x_0 + \frac{b}{d}n\right) + b\left(y_0 - \frac{a}{d}\right)n$$

$$= ax_0 + \frac{ab\cancel{n}}{\cancel{d}} + by_0 - \frac{ba\cancel{n}}{\cancel{d}}$$

$$= ax_0 + by_0$$

$$= ase + bte$$

$$= c$$

$\therefore$ $x = x_n$, $y = y_n$ is a solution for each n.

It is clear that, for different values of n, the solutions (x_n, y_n) are different.

Finally, we show that any solution is of the form

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

Suppose $x = u$, $y = v$ is any solution.
Then,

$$au + bv = c.$$

Also, $ax_0 + by_0 = c$.

$$\therefore \quad au + bv = ax_0 + by_0.$$

$$\therefore \quad a(u - x_0) = b(y_0 - v) \quad \text{—— } (1)$$

$$\therefore \quad \frac{a}{d}(u - x_0) = \frac{b}{d}(y_0 - v)$$

$\therefore \frac{a}{d}$ divides $\frac{b}{d}(y_0 - v)$.

But $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ (by Theorem 3.6)

$\therefore \frac{a}{d}$ divides $y_0 - v$ (by Lemma 3.4)

$\therefore y_0 - v = \frac{a}{d} n$ for some $n \in \mathbb{Z}$.

$\therefore v = y_0 - \left(\frac{a}{d}\right) n$.

Substitute this v value in 1 to get

$a(u - x_0) = b\left(\frac{a}{d}\right) n$

$\therefore u = x_0 + \left(\frac{b}{d}\right) n$

Hence the result.

ex: $12x + 20y = 9$ has no solutions since

$\gcd(12, 20) = 4$ and $4 \nmid 9$.

ex: $21x + 14y = 70$ has infinitely many solutions since $\gcd(21, 14) = 7$ and $7 \mid 70$.

$21x + 14y = 70$ is equivalent to

$3x + 2y = 10$

By Euclidean algorithm,

$$3 = 2\cdot 1 + 1$$

$\therefore\ 3\cdot 1 + 2\cdot(-1) = 1$

$\therefore\ 3(10) + 2(-10) = 10$

$\therefore\ x = 10,\ y = -10$ is a solution.

$\therefore$ all solutions are given by

$x = 10 + 2n,\ y = -10 - 3n$

In particular, if we need positive solutions, we should have

$$10 + 2n > 0 \text{ and } -10 - 3n > 0$$

$\iff\ n > -5$ and $n < -10/3$

$\iff\ -5 < n < -10/3$

Hence, $n = -4$ gives the only positive solution. It is $x = 2$ and $y = 2$.

The above theorem can be extended to any number of variables.

<u>Theorem 3.24:</u> Let $a_1, a_2, \ldots, a_n$ be nonzero integers. Then the equation $a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$ has a solution if and only if $d = (a_1, a_2, \ldots, a_n)$ divides c. Moreover, if there is a solution, then there are infinitely many solutions.

Proof: Exercise

ex: Solve $74x + 35y = 125$.