4. Linear Diophantine Equations

Lemma 4.1. *There are no integers m and n such that*

$$15m + 35n = 121.$$

Proof. Suppose not, suppose there were integers m and n such that $15m + 35n = 121$.

Note that

$$\begin{aligned} 15m + 35n &= 5 \cdot 3m + 5 \cdot 7n \\ &= 5(3m + 7n). \end{aligned}$$

As $3m + 7n$ is an integer, it follows that 5 divides $15m + 35n$. Thus the LHS of the equation

$$15m + 35n = 121$$

is divisible by 5. It follows that 5 divides 121. Thus there is an integer k such that

$$121 = 5k.$$

Suppose that $k \leq 24$. Then

$$\begin{aligned} 5k &\leq 5 \cdot 24 \\ &= 120 \\ &< 121. \end{aligned}$$

On the other hand, if $k \geq 25$ then

$$\begin{aligned} 5k &\geq 5 \cdot 25 \\ &= 125 \\ &> 121. \end{aligned}$$

Since any integer is either at most 24 or at least 25, it follows that there is no integer k such that $121 = 5k$. This is a contradiction. This contradiction arose from the assumption that there are integers integers m and n such that $15m + 35n = 121$.

It follows that there are no integers m and n such that

$$15m + 35m = 121. \qquad \square$$

Note that we introduced a new proof technique in the last proof, proof by contradiction. We wanted to prove the non-existence of integers m and n. We supposed the opposite, that there were integers m and n with a given property. Based on this assumption, correctly applying the basic rules of arithmetic, we arrived at a statement which is palbably false. Since truths only lead to truths, our original assumption had to be have been false. But then what we wanted to be true is true.

Proposition 4.2. *Let a and b be any two integers.*

If there is an integer $d > 1$ such that d divides a and d divides b then the equation

$$ax + by = 1$$

has no integer solutions for x and y.

Proof. Suppose not, suppose by way of contradiction there were integers m and n such that

$$am + bn = 1.$$

By assumption d divides a so that $a = da_1$ for some integer a_1. Similarly, by assumption d divides b so that $b = db_1$ for some integer b_1. Note that

$$\begin{aligned} am + bn &= d \cdot a_1 m + d \cdot b_1 n \\ &= d(a_1 m + b_1 n). \end{aligned}$$

As $a_1 m + b_1 n$ is an integer, it follows that d divides $am + bn$. Thus the LHS of the equation

$$am + bn = 1$$

is divisible by d. It follows that d divides 1. (3.5) implies that $d \leq 1$. This is a contradiction. This contradiction arose from the assumption that there are integers integers m and n such that $am + bn = 1$.

It follows that there are no integers m and n such that

$$am + bn = 1. \qquad \square$$