Exercise 1.5

We are supposing that

$$\gcd(m, n) = 1 \text{ and } 0 < N < mn,$$

and we are looking for solutions of

$$mx + ny = N$$

with $x, y \geq 0$.

It is worth noting that this equation has at most one such solution. For evidently

$$0 \leq x < n, \ 0 \leq y < m.$$

If now $(x_1, y_1),)(x_2, y_2)$ are two solutions then

$$m(x_1 - x_2) = n(y_2 - y_1);$$

and so (since $\gcd(m, n) = 1$)

$$n \mid x_1 - x_2 \implies x_1 = x_2 \implies y_1 = y_2.$$

To try to find a solution, we repeatedly subtract m from N, going through the n numbers

$$N, N - m, N - 2m, \ldots, N - m(n-1),$$

until we meet a number that is a multiple of n.

Note that the numbers in this sequence have different remainders modulo n. For if $N - rm$ and $N - sm$ have the same remainder then

$$n \mid (r - s)m \implies n \mid r - s \implies r = s.$$

In particular, we must reach a number with remainder 0, ie divisible by n.

We see that there is a solution with $x, y \geq 0$ if and only if this multiple of n, say sn, is reached while $N - tm \geq 0$; for then

$$N = mt + ns.$$

If

$$N \geq m(n-1)$$

then this will certainly be the case, since all n numbers $N - tm$ will be ≥ 0.

But we can go further. If $N - tm < 0$ the first time a multiple of n is encountered, then we must have

$$N - tm = -n.$$

It follows that

$$N - (n-1)m \leq -n.$$

ie

$$N \leq (n-1)m - n = mn - (m+n);$$

and we see that for this value of N there is no solution with $x, y \geq 0$.

We conclude that the greatest number N not expressible in the form

$$N = mx + ny$$

is

$$N = mn - (m+n).$$

For suppose there are two solutions, We can suppose that $x_1 <= x_2$. Then

$$mx_1 + ny_1 = N = mx_2 + ny_2,$$

and so

$$m(x_2 - x_1) = n(y_1 - y_2).$$

Since $\gcd(m, n) = 1$ it follows that

$$n \mid x_2 - x_1.$$

But $x_1, x_2 < n$. It follows that $x_1 = x_2$ and so also $y_1 = y_2$.

Of course there may be no solution, eg if $r = 1$ and $m, n \geq 2$ then there is obviously no solution.

On the other hand, suppose $m < n$ and suppose

$$m(n-1) \leq N < mn.$$

Then we can find a solution as follows. Subtract m repeatedly from N, to give the n numbers

$$N, N - m, N - 2m, \ldots, N - m(n-1).$$

These numbers all have different remainders $\bmod n$. For suppose $N - rm, N - sm$ have the same remainder. Then

$$n \mid m(r - s) \implies n \mid r - s,$$

which is impossible unless $r = s$ since $0 \leq r, s < n$. It follows that one of these numbers, say $N - rm$, has remainder 0, ie

$$N - rm = nq \implies N = mr + nq.$$