

THE JOY OF NUMBERS

1. THE LAST WORD ON THE EQUATION $ax + by = c$.

In the first part of class we discussed the test. In particular we proved all together the claim in 2(a).

We then summarized at what point we are with the equation $ax + by = c$. We recalled that we know that there exists a solution if and only if $d = \gcd(a, b)$ divides c .

The next task is to list all the possible solutions given one. In particular, we want to prove the following

(1.1) Theorem. *Let a, b and c be integers. Let (x_0, y_0) be a solution of the equation $ax + by = c$. Then (x_1, y_1) is a solution for the equation $ax + by = c$ if and only if there exists an integer n such that $x_1 = x_0 - \frac{b}{d}n$ and $y_1 = y_0 + \frac{a}{d}n$.*

Proof. (Alex writes but everybody is helping) There are two things to prove: first if there exists an integer n such that $x_1 = x_0 - \frac{b}{d}n$ and $y_1 = y_0 + \frac{a}{d}n$, then (x_1, y_1) is a solution of the equation $ax + by = c$: indeed

$$\begin{aligned} ax_1 + by_1 &= a\left(x_0 - \frac{b}{d}n\right) + b\left(y_0 + \frac{a}{d}n\right) \\ &= ax_0 + by_0 - \frac{ab}{d}n + \frac{ab}{d}n \\ &= ax_0 + by_0 = c, \end{aligned}$$

where the last equality follows because we know that (x_0, y_0) is a solution of the equation $ax + by = c$.

On the other hand, let (x_1, y_1) be a solution of the equation $ax + by = 0$, we want to show that there exists an integer n such that $x_1 = x_0 - \frac{b}{d}n$ and $y_1 = y_0 + \frac{a}{d}n$. For example if the equation we are looking at is $6x + 8y = 20$ and $(2, 1)$ and $(-2, 4)$ are two solutions. Then $-2 = 2 - 4(1)$, $4 = 1 + 3(1)$.

What we know is

$$(1.1.1) \quad ax_0 + by_0 = c$$

and

$$(1.1.2) \quad ax_1 + by_1 = c$$

By subtracting (1.1.2) to (1.1.1), we obtain that

$$a(x_0 - x_1) + b(y_0 - y_1) = 0.$$

Let write $a = dr$ and $b = ds$, we know from a previous homework that $\gcd(r, s) = 1$. By substituting back in the equation, we obtain:

$$\begin{aligned} a(x_0 - x_1) &= b(y_1 - y_0) \\ dr(x_0 - x_1) &= ds(y_1 - y_0) \end{aligned}$$

$$r(x_0 - x_1) = s(y_1 - y_0).$$

From the next lemma we know that $r|(y_1 - y_0)$ and $s|(x_0 - x_1)$. Let us denote by n the integer $\frac{y_1 - y_0}{r} = \frac{x_0 - x_1}{s}$; we obtain

$$\begin{aligned} nr &= y_1 - y_0, & ns &= x_0 - x_1 \\ y_1 &= y_0 + nr, & x_1 &= x_0 - ns \\ y_1 &= y_0 + n\frac{b}{d} & x_1 &= x_0 - n\frac{a}{d} \end{aligned}$$

□

Chris answered a question of Sara.

(1.2) **Proposition.** *Let a, b, c be integers. Assume that $(x_0, y_0), (x_1, y_1)$ are solutions of the equation $ax + by = c$. The sets*

$$\begin{aligned} S_0 &= \{(x, y) \mid x = x_0 - \frac{b}{d}n, \quad y = y_0 + \frac{a}{d}n\} \\ S_1 &= \{(x, y) \mid x = x_1 - \frac{b}{d}n, \quad y = y_1 + \frac{a}{d}n\} \end{aligned}$$

are the same.

Proof. By the above theorem, we know that all the solutions of the equation $ax + by = c$ belong to the set S_0 , in particular there exists an integer n_1 such that $x_1 = x_0 - \frac{b}{d}n_1$ and $y_1 = y_0 + \frac{a}{d}n_1$. We will show that an element of the set S_1 is also an element in the set S_0 . Pick an element (\bar{x}, \bar{y}) of S_2 , we can write

$$\bar{x} = x_1 - \frac{b}{d}n, \quad \bar{y} = y_1 + \frac{a}{d}n,$$

for some n . If we substitute x_1 and y_1 in terms of x_0 and y_0 , to obtain

$$\begin{aligned} \bar{x} &= x_1 - \frac{b}{d}n = x_0 - \frac{b}{d}n_1 - \frac{b}{d}n \\ &= x_0 - \frac{b}{d}(n_1 + n) \\ \bar{y} &= y_1 + \frac{a}{d}n = y_0 + \frac{a}{d}n_1 + \frac{a}{d}n \\ &= y_0 + \frac{a}{d}(n_1 + n), \end{aligned}$$

showing that there is an integer $(n_1 + n)$ that makes (\bar{x}, \bar{y}) an element of the set S_0 . In the same way, we can prove that every element in S_0 is in the set S_1 . □

We left class with a Homework:

(1.3) **Exercise.** Let r, s, a, b be integers such that $\gcd(r, s) = 1$ and $ra = sb$. Show that $r|a$ and $s|b$.