

## THE JOY OF NUMBERS

### 1. PROOF OF THE DIVISION THEOREM

Kevin presented us the proof of the Division Theorem:

(1.1) **Theorem.** *Let  $a$  and  $b$  be two integers such that  $b > 0$  and  $a \geq b$ . There exists two unique integers  $q$  and  $r$  such that  $a = bq + r$  and  $0 \leq r < b$ .*

*Proof.* Let  $S$  denote the set of all (integer) multiples of  $b$  which are less than or equal to  $a$ . As an example, if  $a = 20$  and  $b = 6$  then  $S = \{18, 12, 6, 0, -6, -12, \dots\}$ . By the well-ordering axiom,  $S$  must have a greatest element, call it  $p$ . Then  $p = bq$  for some  $q \in \mathbb{Z}$  and  $p \leq a$ . Let  $r = a - p$ . Then  $a = p + r = bq + r$ . Since  $a \geq p$  we see that  $r \geq 0$ . We prove  $r < b$  by contradiction. Suppose  $r \geq b$ . Then  $a - b(q + 1) = a - bq - b = r - b \geq 0$ . If we let  $p' = b(q + 1)$ , we see that  $p' \leq a$ . Since  $p'$  is clearly a multiple of  $b$ , we get that  $p' \in S$ . But  $p' = b(q + 1) > bq = p$ , contradicting that  $p$  is the largest element of  $S$ . Thus, we must have  $r < b$ .

This proves the *existence* of the integers  $q$  and  $r$ . Equally important is the *uniqueness* of  $q$  and  $r$ . That is, there are no other integers  $s$  and  $t$  such that  $a = bs + t$  with  $0 \leq t < b$ . We didn't have time to prove this in class, but we give the proof here for completeness. Suppose the integers  $s$  and  $t$  also work: i.e.,  $a = bs + t$  with  $0 \leq t < b$ . We will show that  $q = s$  and  $r = t$ , so that  $q$  and  $r$  are the only integers which work. We can start by saying that  $a = bq + r = bs + t$ , so that  $bq - bs = t - r$ . This means that  $b$  divides  $t - r$ . By the restriction of the sizes of  $r$  and  $t$ , we know that  $-(b - 1) \leq t - r \leq b - 1$ . The only integer in this range which is divisible by  $b$  is 0, so we must have  $t - r = 0$ . In other words, we have  $t = r$ . But then we have  $a = bq + r = bs + t = bs + r$ , so  $bq = bs$ , which means that  $q = s$ , finishing the proof of the uniqueness part of the theorem.  $\square$

### 2. ON THE EQUATION $ax + by = c$

The problem of the king of Nobeh, brought us to discuss the equation  $ax + by = c$ . We have identified two issues:

- (1) Given the equation  $ax + by = c$ , when there are integer solutions? Otherwise said, when can we find two integers  $x_0$  and  $y_0$  such that  $ax_0 + by_0 = c$ ?
- (2) Given a solution  $(x_0, y_0)$  how can we describe all the solutions of the equation  $ax + by = c$ ?

We completely answered the first question:

(2.1) **Theorem.** *The equation  $ax + by = c$  has an integer solution if and only if  $\gcd(a, b)$  divides  $c$ .*

*Proof.* Let  $d = \gcd(a, b)$ , if  $d|c$  then we used the back substitution method: see the example below.

Assume that there exists two integers  $x_0$  and  $y_0$  such that  $ax_0 + by_0 = c$ . Let  $h$  and  $k$  be two integers such that  $a = hd$  and  $b = kd$ , then

$$c = ax_0 + by_0 = hdx_0 + kdy_0 = d(hx_0 + ky_0)$$

showing that  $d$  divides  $c$ . □

(2.2) **Example.** This is our last example on how to find an integer solution of the equation  $ax + by = c$  if the  $\gcd(a, b)$  divides  $c$ .

Let consider the equation  $40x + 25y = 10$ . We know that there is a solution since  $\gcd(40, 25) = 5$  and 5 divides 10. From

$$\begin{aligned} 40 &= 25 + 15 \\ 25 &= 15 + 10 \\ 15 &= 10 + 5 \\ 10 &= (2)(5) + 0 \end{aligned}$$

By using Back substitution we will get

$$\begin{aligned} 5 &= 15 - 10 \\ &= 15 - (25 - 15) \\ &= (2)(15) - 25 \\ &= (2)(40 - 25) - 25 \\ &= (2)(40) - (3)(25) \end{aligned}$$

Therefore  $10 = (4)(40) - (6)(25)$ .

We then returned to the second question. I put up the example from last time and Jay gave conjectures on how to describe all the possible solutions of  $ax + by = c$ :

|   | Equation     | particular solution | general solution |
|---|--------------|---------------------|------------------|
| 1 | $3x+5y=22$   | $(-1,5)$            | $(-1-5n,5+3n)$   |
| 2 | $6x+8y=20$   | $(2,1)$             | $(2-8n,1+6n)$    |
| 3 | $3x+2y=17$   | $(1,7)$             | $(1-2n,7+3n)$    |
| 4 | $12x+15y=39$ | $(2,1)$             | $(2+5n,-1-4n)$   |

It seems that the proposed pattern is that if  $(x_0, y_0)$  is a solution of  $ax + by = c$  then all the others can be written as  $(x_0 - bn, y_0 + an)$ .

We noticed that for example (2)  $(-2, 4)$  is a solution but it can not be written as  $(2 - 8n, 1 + 6n)$  for any integer  $n$ . So we need to change conjecture:

(2.3) **Conjecture.** (Alex) If  $(x_0, y_0)$  is a solution of  $ax + by = c$ , then all the other solutions are given by  $(x_0 - \frac{b}{d}n, y_0 + \frac{a}{d}n)$  for any integer  $n$ , where  $d = \gcd(a, b)$ .

Sara Came up with the following question:

(2.4) **Question.** Does it matter with which solution do we start? If  $(x_1, y_1)$  is another solution, is the set  $(x_0 - \frac{b}{d}n, y_0 + \frac{a}{d}n)$  and  $(x_1 - \frac{b}{d}n, y_1 + \frac{a}{d}n)$  the same?