MATHEMATICS 300 — SPRING 2019

Introduction to Mathematical Reasoning

H. J. Sussmann

HOMEWORK ASSIGNMENT NO. 3, DUE ON WEDNESDAY, FEBRUARY 23, FOR SECTION 9, AND ON THURSDAY, FEBRUARY 28, FOR SECTION 2

*This homework consists of a list of **eight** problems. These problems are all related, and follow a logical progression, so I strongly recommend that you do them all, in order. But I am only asking you to hand in **four** of them. The list of four problems to hand in is given below.*

Problems to hand in: 5, 6, 7, 8.

Problem 1. This problem is about the following question: *for which real numbers a does the equation*

$$ax = b \tag{1}$$

have a real solution[1] *for every real number c?*

We want a necessary and sufficient condition in terms of the real number a for it to be true that

$$(\forall b \in \mathbb{R})(\exists x \in \mathbb{R})ax = b\,. \tag{2}$$

Prove that the condition "$a \neq 0$" is necessary and sufficient for (2) to be true. That is, prove the following:

$$(\forall a \in \mathbb{R})\Big((\forall b \in \mathbb{R})(\exists x \in \mathbb{R})ax = b \iff a \neq 0\Big)\,. \tag{3}$$

Problem 2. This problem is about the same question as Problem 1, but over the integers rather than over the real numbers.

We want to know: *for which integers a does the equation*

$$ax = b \tag{4}$$

[1] A real solution of (1) is an x such that $x \in \mathbb{R}$ and (1) holds.

have an integer solution[2] *for every integer* b*?*

We want a necessary and sufficient condition in terms of the integer a for it to be true that

$$(\forall b \in \mathbb{Z})(\exists x \in \mathbb{Z})ax = b\,. \tag{5}$$

The answer turns out to be: the necessary and sufficent condition is "$a = 1 \vee a = -1$". (If you prefer, you can rewrite this condition as "$|a| = 1$", or as "$a^2 = 1$".)

Prove that the condition "$a = 1 \vee a = -1$" is necessary and sufficient for (5) to be true. That is, prove the following:

$$(\forall a\in\mathbb{Z})\Big((\forall b\in\mathbb{Z})(\exists x\in\mathbb{Z})ax = b \Longleftrightarrow (a = 1 \vee a = -1)\Big)\,. \tag{6}$$

Problem 3. This problem is about the following question: *for which real numbers* a, b *does the equation*

$$ax + by = c \tag{7}$$

have a real solution[3] *for every real number* c*?*

We want a necessary and sufficient condition in terms of the real numbers a, b for it to be true that

$$(\forall c \in \mathbb{R})(\exists x \in \mathbb{R})(\exists y \in \mathbb{R})ax + by = c\,. \tag{8}$$

(I) Prove that the condition "$a \neq 0 \vee b \neq 0$" is necessary and sufficient for (8) to be true. That is, prove the following:

$$(\forall a\in\mathbb{R})(\forall b\in\mathbb{R})\Big((\forall c\in\mathbb{R})(\exists x\in\mathbb{R})(\exists y\in\mathbb{R})ax+by = c \Longleftrightarrow (a \neq 0\vee b \neq 0)\Big)\,. \tag{9}$$

Problem 4. Consider the sentence

$$(\forall a\in\mathbb{R})(\forall b\in\mathbb{R})(\forall c\in\mathbb{R})(\exists x\in\mathbb{R})(\exists y\in\mathbb{R})\Big(ax + by=c\Longleftrightarrow(a\neq0\vee b\neq0)\Big)\,. \tag{10}$$

(This looks "almost the same" as (9), but it is very different!)

1. ***Translate*** (10) into English.

[2] An integer solution of (4) is an x such that $x \in \mathbb{Z}$ and (4) holds.

[3] A real solution of (7) is a pair (x, y) such that $x \in \mathbb{R}$, $y \in \mathbb{R}$, and (7) holds.

2. ***Indicate*** whether (10) is true or false, and ***prove*** your statement.

Problem 5. This problem is about the same question as Problem 3, but over the integers rather than over the real numbers.

We want to know: *for which integers a, b does the equation*

$$ax + by = c \tag{11}$$

have an integer solution[4] *for every integer c?*

We want a necessary and sufficient condition in terms of the integers a, b for it to be true that

$$(\forall c \in \mathbb{Z})(\exists x \in \mathbb{Z})(\exists y \in \mathbb{Z})ax + by = c\,. \tag{12}$$

The asnwer turns out to be more complicated than that of Problem 1.

First you should review the definition of "coprime integers", and the notation "$a \perp b$", explained in the Appendix, on page 6.

It turns out that

- The necessary and sufficient condition that we are looking for is the following: "$a \perp b$". The actual result is:

  Theorem. *If a, b are integers, then the equation "$ax + by = c$" has am integer solution for every integer c if and only if a and b are coprime.*

  In formal language, the theorem says that

  $$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})\Big((\forall c \in \mathbb{Z})(\exists x \in \mathbb{Z})(\exists y \in \mathbb{Z})ax + by = c \Longleftrightarrow a \perp b\Big)\,. \tag{13}$$

- Proving this theorem is not very easy. Half of it (the implication "$(\forall c \in \mathbb{Z})(\exists x \in \mathbb{Z})(\exists y \in \mathbb{Z})ax + by = c \Longrightarrow a \perp b$") is quite easy. But the other part (the implication "$a \perp b \Longrightarrow (\forall c \in \mathbb{Z})(\exists x \in \mathbb{Z})(\exists y \in \mathbb{Z})ax + by = c$") is much harder, and requires a very powerful result called "Bézout's Lemma". But I am going to make it easy for you by allowing yoo to use Bézout's Lemma.

  And, in order to get you to appreciate the depth and power of Bézout's Lemma, I will ask you to verify the result for a few values of a and b.

[4] An integer solution of (11) is a pair (x, y) such that $x \in \mathbb{Z}$, $y \in \mathbb{Z}$, and (11) holds.

(I) Prove that the condition "$a \perp b$" is necessary and sufficient for (12) to be true. That is, prove the following:

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})\Big((\forall c \in \mathbb{Z})(\exists x \in \mathbb{Z})(\exists y \in \mathbb{Z})ax + by = c \iff a \perp b\Big). \qquad (14)$$

(That is: *if a and b are integers such that for every integer c the equation "$ax + by + c$" has an integer solution, then a and b are coprime. And, conversely, if a and b are coprime integers then for every integer c the equation "$ax + by + c$" has an integer solution.*)

A VERY IMPORTANT HINT. Use Bézout's Lemma. (See page 7 below. We will prove Bézout's Lemma later in the course.))

A COMMENT. Proving (14) is hard. I am making it easy for you by allowing you to use Bézout's Lemma. Actually, statement (14) is almost the same as Bézout's Lemma, so I am essentially giving you this problem for free.

ANOTHER COMMENT. Bézout's Lemma is one of the most important and powerful results in integer arithmetic. Actually, all of integer arithmetic is based on the systematic use of two results: the division theorem and Bézout's Lemma.

A RECOMMENDATION. Read the *Wikipedia* article on "Bézout's identity".

(II) Verify directly. without using (14) or Bézout"s Lemma, that the implication

$$a \perp b \Longrightarrow (\forall c \in \mathbb{Z})(\exists x \in \mathbb{Z})(\exists y \in \mathbb{Z})ax + by = c \qquad (15)$$

is true for the following values of a and b:

1. $a = 2$, $b = 3$,
2. $a = 6$, $b = 12$,
3. $a = 5$, $b = 7$,
4. $a = 6$, $b = 12$,
5. $a = 3$, $b = 7$,
6. $a = 41$, $b = 43$,
7. $a = 23$, $b = -39$,

8. $a = -60$, $b = -37$,

9. $a = 913$, $b = 77$.

(If you want an idea of how this is done, look at Examples 1, 2, 3, 4 in the Appendix.)

Problem 6. ***Find*** all the integer solutions of the equation

$$65x + 28y = 1\,. \tag{16}$$

(HINT. Remember the words that you must have seen at least once: *the general solution of an inhomogeneous equation is the sum of a particular solution of the inhomogeneous equation plus the general solution of the associated homogeneous equation.*) □

Problem 7. This problem is about the following question: *for which real numbers a, b, c, d does the system of equations*

$$ax + by = e\,, \tag{17}$$
$$cx + dy = f \tag{18}$$

have a real solution[5] *for every pair of real numbers e, f?*

We want a necessary and sufficient condition in terms of the real numbers a, b, c, d for it to be true that

$$(\forall e \in \mathbb{R})(\forall f \in \mathbb{R})(\exists x \in \mathbb{R})(\exists y \in \mathbb{R})(ax + by = e \wedge cx + dy = f)\,. \tag{19}$$

Prove that the condition "$ad - bc \neq 0$" is necessary and sufficient for (19) to be true. That is, prove the following:

$$(\forall a \in \mathbb{R})(\forall b \in \mathbb{R})(\forall c \in \mathbb{R})(\forall d \in \mathbb{R})\Bigg((\forall e \in \mathbb{R})(\forall f \in \mathbb{R})$$
$$(\exists x \in \mathbb{R})(\exists y \in \mathbb{R})(ax + by = e \wedge cx + dy = f) \Longleftrightarrow ad - bc \neq 0\Bigg)\,. \tag{20}$$

[5] A real solution of the system (17), (18) is a pair (x, y) such that $x \in \mathbb{R}$, $y \in \mathbb{R}$, and the equations (17, (18) hold.

Problem 8. *This problem is about the same question as Problem 7, but over the integers rather than over the real numbers.*

We want to answer the following question: *for which integers a, b, c, d does the system of equations*

$$ax + by = e\,, \tag{21}$$
$$cx + dy = f \tag{22}$$

have an integer solution[6] *for every pair of integers e, f?*

We want a necessary and sufficient condition in terms of the integers a, b, c, d for it to be true that

$$(\forall e \in \mathbb{Z})(\forall f \in \mathbb{Z})(\exists x \in \mathbb{Z})(\exists y \in \mathbb{Z})(ax + by = e \wedge cx + dy = f)\,. \tag{23}$$

Prove that the condition[7] "$ad - bc = 1 \vee ad - bc = -1$" is necessary and sufficient for (23) to be true. That is, prove the following:

$$(\forall a\in\mathbb{Z})(\forall b\in\mathbb{Z})(\forall c\in\mathbb{Z})(\forall d\in\mathbb{Z})\Bigg((\forall e\in\mathbb{Z})(\forall f\in\mathbb{Z})$$
$$(\exists x\in\mathbb{Z})(\exists y\in\mathbb{Z})(ax+by=e\wedge cx+dy=f)\iff ad-bc\neq 0\Bigg)\,. \tag{24}$$

Appendix: Review of definitions and some examples

Coprime integers

Definition. Two integers a, b are coprime if the only natural number that divides both a and b is the number 1. (That is, a and b are coprime if they have no positive common factors other than 1.)
We write "$a \perp b$" for "a and b are coprime". Then

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})\Big(a \perp b \iff (\forall k \in \mathbb{N})\big((k|a \wedge k|b) \implies k = 1\big)\Big)\,. \tag{25}$$

[6] A integer solution of the system (21), (22) is a pair (x, y) such that $x \in \mathbb{Z}$, $y \in \mathbb{Z}$, and the equations (21), (22) hold.

[7] Instead of "$ad - bc = 1 \vee ad - bc = -1$" we could have written "$|ad = bc| = 1$", or "$(ad = bc)^2 = 1$". These are different ways of saying example the same thing.

The division theorem

Theorem. *Let a, b be integers such that $b \neq 0$. Then there exist unique integers q, r such that*

$$a = bq + r \text{ and } 0 \leq r < |b| .$$

Bézout's Lemma

Theorem. *Let a, b be integers with greatest common divisor g. Then there exist integers x and y such that $ax + by = g$. More generally, the integers of the form $ax + by$ are exactly the integer multiples of g.*

Example 1. Let us show how to find an integer solution of the equation

$$65x + 28y = c . \tag{26}$$

for every integer c.

The trick is to first find an integer solution of the equation

$$65x + 28y = 1 , \tag{27}$$

and then multiply by c to get a solution of (26).

In order to find an integer solution of (27), we use another trick: we find integer solutions of equations $65x + 21y = c$ for smaller and smaller c, and try to make c as small as possible, until we end up with $c = 1$, if we can.

To get started, observe that $2 \times 28 = 56$, which is close to 65. Then

$$65 \times 1 + 28 \times (-2) = 9 . \tag{28}$$

So if $c = 9$ then the equation $65x + 28y = c$ has an integer solution, namely, $x = 1$, $y = -2$.

Now let us try to get a smaller c for which the equation $65x + 28y = c$ has an integer solution.

We multiply both sides of (28) by[8] 3 we get

$$65 \times 1 \times 3 + 28 \times (-2) \times 3 = 9 \times 3 , \tag{29}$$

[8]Why do I choose to multply by 3? Because 9×3 is 27, which is pretty close to 28.

that is,

$$65 \times 3 + 28 \times (-6) = 27\,. \tag{30}$$

But $27 = 28 - 1$, so

$$65 \times 3 + 28 \times (-6) = 28 - 1\,, \tag{31}$$

and then

$$65 \times 3 + 28 \times (-6) - 28 = -1\,, \tag{32}$$

that is,

$$65 \times 3 + 28 \times (-7) = -1\,, \tag{33}$$

and then

$$65 \times (-3) + 28 \times 7 = 1\,. \tag{34}$$

So we have found an integer solution of (27), namely, $x = -3$, $y = 7$.

Verification[9]: $65 \times 3 = 195$, so $65 \times (-3) = -195$. And $28 \times 7 = 196$. So $65 \times (-3) + 28 \times 7 = 196 - 195$, and then $65 \times (-3) + 28 \times 7 = 1$. So our solution works.

Then, if c is an arbitrary integer, we can find a solution of (26) by just multiplying both sides of (27) by c. We get

$$65 \times (-3c) + 28 \times 7c = c\,. \tag{35}$$

Therefore: *for every integer c, the equation "*$65x + 28y = c$*" has a solution. namely,* $x = -3c$, $y = 7c$. □

Example 2. Let us verify the conclusion of Bézout's Lemma for $a = 6$, $b = 14$.

Clearly, the greatest common divisor g is 2. Bézout's Lemma says that The equation

$$6x + 14y = 2$$

has an integer solution. (That is, there exist integers x, y such that $6x + 14y = 2$.) And, indeed, this is true. (Proof: Take $x = -2$, $y = 1$. Then $6x + 14y = 2$).

[9]When you solve an equation or system of equations, ***you should always verify that what you think is the solution actually does satisfy the equation or system***, because (a) it's easy to make a mistake in your calculation, (b) if your derivation, what you have really shown is that ***if*** x (or x, y) is a soluton then it must be equal to something. That does not imply that x (or (x, y)) ***is*** a solution.

Example 3. According to Bézout's Lemma, the equation

$$6x + 14y = 1$$

should not have an integer solution, because $g = 2$, so the values of c for which $6x + 14y = c$ has a solution are the multiples of 2, i.e., the even numbers, and 1 is not even.

And, indeed, there do not exist integers x, y such that $6x + 14y = 1$. (Proof: If x, y are arbitrary inetegrs, then $6x + 15y$ is even. So $6x + 15y$ cannot possible ne equal to 1.)

Example 4. Let $a = 45$, $b = 73$. Then $g = 1$. The equation

$$45x + 73y = 1$$

has an integer solution. That is, there exist integers x, y such that $45x+73y = 1$.

Let us find a solution. First: if we take $x = 2$, $y = -1$, we get

$$45 \times 2 + 73 \times (-1) = 17\,,$$

so we have a solution of $45x + 73y = 17$. That's not quite the equation $45x + 73y = 1$, but it's step toward that equation.

Next, divide 45 by 17. The quotient is 2 and the remainder is 11, so $45 = 17 \times 2 + 11$, and then $45 - 17 \times 2 = 11$. But $17 = 45 \times 2 + 73 \times (-1)$, so

$$\begin{aligned} 11 &= 45 - 17 \times 2 \\ &= 45 - \Big(45 \times 2 + 73 \times (-1)\Big) \times 2 \\ &= 45 - 45 \times 2 \times 2 - 73 \times (-1) \times 2 \\ &= 45 - 45 \times 4 + 73 \times 2 \\ &= 45 \times (-3) + 73 \times 2\,. \end{aligned}$$

That is:

$$45 \times (-3) + 73 \times 2 = 11\,.$$

So we have a solution of $45x + 73y = 11$. That's not quite the equation $45x + 73y = 1$, but it's step toward that equation, and it's better than $45x + 73y = 17$. Next, divide 45 by 11. The quotient is 4 and the remainder

is 1, so $45 = 11 \times 4 + 1$, and then $45 - 11 \times 4 = 1$. But $11 = 45 \times (-3) + 73 \times 2$, so

$$\begin{aligned} 1 &= 45 - 11 \times 4 \\ &= 45 - \Big(45 \times (-3) + 73 \times 2\Big) \times 4 \\ &= 45 - 45 \times (-3) \times 4 - 73 \times 2 \times 4 \\ &= 45 + 45 \times 12 - 73 \times 8 \\ &= 45 \times 13 - 73 \times 8 \end{aligned}$$

, .

Hence $\boxed{\boxed{45 \times 13 + 73 \times (-8) = 1}}$, and we have found an integer solution of $45x + 73y = 1$, namely, $x = 13$, $y = -8$. (***Verification:*** $45 \times 13 = 585$, and $73 \times 8 = 584$.)