MATHEMATICS 300 — FALL 2018

Introduction to Mathematical Reasoning

H. J. Sussmann

HOMEWORK ASSIGNMENT NO. 5, DUE ON THURSDAY, OCTOBER 25 (FOR SECTION 5) AND FRIDAY, OCTOBER 26 (FOR SECTION 3)

This assignment consists of just one problem.

Problem. *This problem proposes a different proof and a generalization of the theorem that says that the greatest common divisor of two integers a, b is the smallest positive integer linear combination of a and b.*

Definition 1. If $n \in \mathbb{N}$, and $a_1, a_2, \ldots, a_n$ are integers, an integer g is a <u>greatest common divisor</u> (GDC) of $a_1, a_2, \ldots, a_n$ if

1. g divides all the a_js (that is: $(\forall j \in \mathbb{N})(j \leq n \Longrightarrow g|a_j)$).
2. if c is any integer such that c divides all the a_js, then $c \leq g$. (That is: $(\forall c \in \mathbb{Z})\Big((\forall j \in \mathbb{N})(j \leq n \Longrightarrow c|a_j) \Longrightarrow c \leq g\Big)$.)

Definition 2. If $n \in \mathbb{N}$, and $a_1, a_2, \ldots, a_n$ are integers, an integer c is an <u>integer linear combination</u> (ILC) of $a_1, a_2, \ldots, a_n$ if

(*) there exist integers $k_1, k_2, \ldots, k_n$ such that

$$c = k_1 a_1 + k_2 a_2 + \cdots + k_n a_n \,.$$

1. ***Prove*** that, if $n \in \mathbb{N}$, and $a_1, a_2, \ldots, a_n$ are integers, then
   (a) If a GCD of $a_1, a_2, \ldots, a_n$ exists, then it is unique. (In view of this, from now on we are entitled to talk about ***the*** greatest common divisor of $a_1, a_2, \ldots, a_n$.)
   (b) If c is a common divisor of the a_j (that is, if $c|a_j$ for $j = 1, 2, \ldots, n$) and b is an integer linear combination of $a_1, a_2, \ldots, a_n$, then c divides b.

(c) If b is an integer linear combination of $a_1, a_2, \ldots, a_n$, b is positive (that is, $b > 0$), and b is not a common divisor of the a_j, then there exists an integer b' such that $0 < b' < b$ and b' is an integer linear combination of $a_1, a_2, \ldots, a_n$. (HINT: Pick j such that b does not divide a_j, and use the division theorem to write $a_j = bq + b'$ with $q, b' \in \mathbb{Z}$ and $0 < b' < b$.)

(d) If all the a_j are equal to zero (that is, if $(\forall j \in \mathbb{N})(j \leq n \Longrightarrow a_j = 0)$), then a GCD of $a_1, a_2, \ldots, a_n$ in the sense of Definition 1 does not exist.

(e) If $a_1, a_2, \ldots, a_n$ are not all equal to zero (that is, if $(\exists j \in \mathbb{N})(j \leq n \wedge a_j \neq 0)$, and S is the set of all positive integers that are ILCs of $a_1, a_2, \ldots, a_n$, then

i. S is nonempty,

ii. the smallest member of S (which exists, because of the Well Ordering Principle) is a GCD of $a_1, a_2, \ldots, a_n$.

2. ***Conclude*** from the above that

(#) If $n \in \mathbb{N}$, and $a_1, a_2, \ldots, a_n$ are integers, then

(a) A GCD of $a_1, a_2, \ldots, a_n$ exists if and only if the a_j are not all equal to zero.

(b) If the a_j are not all equal to zero. then the GCD of $a_1, a_2, \ldots, a_n$ is the smallest of all positive integers that are integer linear combinations of $a_1, a_2, \ldots, a_n$.

3. For $n = 3$, $a_1 = 21$, $a_2 = 60$, $a_3 = 35$, ***find*** the GCD of a_1, a_2, a_3, and ***express it*** as an ILC of a_1, a_2, a_3.