

MATHEMATICS 300 — FALL 2017

Introduction to Mathematical Reasoning

H. J. Sussmann

HOMEWORK ASSIGNMENT NO. 9, DUE ON WEDNESDAY, NOVEMBER 8

The six problems listed here are very important, and you should do them all. But you are only required to hand in four problems, namely, problems 1, 3, 4 and 6. Problem 6 is the most important one, and will be worth 40% of the assignment, whereas the other three problems are worth 20% each.

Some definitions and theorems

Bounded below and bounded above:

Definition 1. If S is a subset of \mathbb{Z} , and b is an integer, we say that b is a lower bound for S if $n \geq b$ for every member n of S . \square

Definition 2. A subset S of \mathbb{Z} is bounded below if it has a lower bound, that is, if there exists an integer b such that

$$(\forall n)(n \in S \implies n \geq b). \quad \square$$

Definition 3. If S is a subset of \mathbb{Z} , and b is an integer, we say that b is an upper bound for S if $n \leq b$ for every member n of S . \square

Definition 4. A subset S of \mathbb{Z} is bounded above if it has an upper bound, that is, if there exists an integer b such that

$$(\forall n)(n \in S \implies n \leq b). \quad \square$$

Coprime integers:

Definition 5. If a, b are integers, we say that a and b are coprime if they have no nontrivial common factors (that is, if the only integers f such that $f|a$ and $f|b$ are 1 and -1). \square

It follows easily from Definition 5 that *if $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$ then a and b are coprime if and only if $GCD(a, b) = 1$.*

A theorem about coprime numbers and divisibility:

Theorem I. If a, b, c are integers such that a and b are coprime and a divides bc , then $a|c$.

Proof. Since a and b are coprime, we can pick integers u, v such that

$$1 = ua + vb.$$

Since $a|bc$, we can pick an integer k such that

$$bc = ka.$$

Then

$$\begin{aligned} c &= 1 \times c \\ &= (ua + vb)c \\ &= uca + vbc \\ &= uca + vka \\ &= (uc + vk)a \end{aligned}$$

so $a|c$.

Q.E.D.

Square-free integers:

Definition 6. An integer n is square-free if there does not exist a natural number m such that $m > 1$ and m^2 divides n . \square

Examples: 33 is square-free, because the only natural numbers that are factors of 33 are 1, 3, 11, and 33, and none of these is a square and > 1 . The number 48 is not square-free, because 48 is divisible by 2^2 . \square

Subgroups of \mathbb{Z} :

Definition 7. Let S be a set of integers, i.e., a subset of \mathbb{Z} . We say that S is a subgroup of \mathbb{Z} if the following two facts are true about S :

- S1. S is nonempty,
- S2. S is closed under subtraction; that is, if a, b are arbitrary members of S , it follows that $a - b \in S$. \square

The homework problems

Problem 1. *Prove* the following statement, that generalizes the well-ordering principle:

[WOPG1] *If S is a nonempty subset of \mathbb{Z} and S is bounded below then S has a smallest member.*

HINT: For an integer k , let us write

$$\mathbb{Z}_{\geq k} = \{n \in \mathbb{Z} : n \geq k\}.$$

So, for example,

1. $\mathbb{Z}_{\geq 3}$ is the set of all integers that are greater than or equal to 3; that is, $\mathbb{Z}_{\geq 3}$ consists of 3, 4, 5, 6, ... and so on.
2. $\mathbb{Z}_{\geq 0}$ is the set of all integers that are greater than or equal to 0; that is, $\mathbb{Z}_{\geq 0}$ consists of 0, 1, 2, 3, 4, 5, ... and so on. In other words, $\mathbb{Z}_{\geq 0} = \mathbb{N} \cup \{0\}$.
3. $\mathbb{Z}_{\geq -5}$ is the set of all integers that are greater than or equal to -5 ; that is, $\mathbb{Z}_{\geq -5}$ consists of $-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, \dots$ and so on.

Prove by induction on n that the following statement $P(n)$ is true for every nonnegative integer (that is, for every n belonging to $\mathbb{N} \cup \{0\}$): *If S is a nonempty subset of $\mathbb{Z}_{\geq -n}$ then S has a smallest member.* You should do this by induction, starting at 0. Here is the base step: we want to prove that $P(0)$ is true. And $P(0)$ says: if S is a nonempty subset of $\mathbb{Z}_{\geq 0}$ then S has a smallest member. To prove this, let S be an arbitrary nonempty subset of $\mathbb{Z}_{\geq 0}$. Then either $0 \in S$ or $0 \notin S$. If $0 \in S$ then 0 is clearly the smallest member of S , because all the members of S are ≥ 0 , since $S \subseteq \mathbb{Z}_{\geq 0}$. If $0 \notin S$ then S is a nonempty subset of \mathbb{N} , so S has a smallest member by the WOP.

You have to do the inductive step.

Problem 2. *Prove* the following statement, which is also a generalization of the WOP:

[WOPG2] *If S is a nonempty subset of \mathbb{Z} and S is bounded above then S has a largest member.*

HINT: Take the set S and “reflect it”, that is, look at the set

$$T = \{n \in \mathbb{Z} : -n \in S\}.$$

Prove that T is bounded below, use the result of Problem 1 to conclude that T has a smallest member, and then draw the conclusion that S has a largest member.

Problem 3. *This problem deals with a result that we have already used many times, for example in the proofs that numbers such as $\sqrt{2}$ or $\sqrt{3}$ are irrational. When we used this result, we did not know how to prove it, because the proof requires the well-ordering principle (WOP). Now that we have the WOP, I am asking you to prove the result.*

Prove that

[*] *If r is a rational number then there exist unique integers m, n such that*

1. $n > 0$,
2. $r = \frac{m}{n}$,
3. m and n are coprime.

(That is, every fraction has a unique **coprime expression**—also called “irreducible expression”, or “expression reduced in lowest terms”—that is, every fraction can be written uniquely as a quotient $\frac{m}{n}$ of integers in such a way that m and n have no common factors and n is positive.)

HINT: Use the WOP. To prove existence, let S be the set of all natural numbers n such that nr is an integer, that is,

$$S = \{n \in \mathbb{N} : nr \in \mathbb{Z}\}.$$

Prove that S is nonempty; then deduce from this, using the WOP, that S has a smallest member n ; then let $m = nr$, so $m \in \mathbb{Z}$ and $r = \frac{m}{n}$; finally, prove that m and n are coprime.

To prove uniqueness, assume that $r = \frac{m_1}{n_1}$ and $r = \frac{m_2}{n_2}$, where m_1, n_1, m_2, n_2 are integers, $n_1 > 0$, and $n_2 > 0$. Prove that $m_1 = m_2$ and $n_1 = n_2$ by observing that $m_1 n_2 = m_2 n_1$ and then, using the fact that n_1 is coprime with m_1 , use Theorem I to conclude that n_1 must divide n_2 . Then prove that n_2 divides n_1 . And, finally, using these two facts, conclude that $n_1 = n_2$.

Problem 4. *Prove* that if n is a natural number then there exist unique natural numbers a, b such that

$$n = 2^{a-1}(2b - 1).$$

HINT: If $n = 1$, the conclusion is easy. If $n \geq 2$, write n as a product $\prod_{k=1}^m p_k$, where p_1, p_2, \dots, p_m are prime numbers such that $p_k \leq p_{k+1}$ for $k = 1, 2, \dots, m - 1$. Let α be the number of factors in this expression that are equal to 2, so $n = 2^\alpha \prod_{k=\alpha+1}^m p_k$. (The number α could be zero, if n is odd.) Let $a = \alpha + 1$.

Problem 5. *Prove* that if n is a natural number then there exist unique natural numbers a, b such that

$$n = a^2b$$

and b is square-free. (The number b is called the square-free part of n .)

Problem 6. *The purpose of this problem is to provide a different proof of Bézout's lemma, based on a theorem on the structure of subgroups of \mathbb{Z} . The definition of "subgroup of \mathbb{Z} " is given above. The theorem that completely determines the structure of all subgroups of \mathbb{Z} is Fact 9 below. Bézout's lemma is Fact 10 below.*

If a is an arbitrary integer, we define a subset $[a]$ of \mathbb{Z} as follows:

$$[a] = \{n \in \mathbb{Z} : (\exists u \in \mathbb{Z})n = ua\}.$$

In other words, $[a]$ is the set of all integers that are multiples of a .

If a, b are arbitrary integers, we define a subset $[a, b]$ of \mathbb{Z} as follows:

$$[a, b] = \{n \in \mathbb{Z} : (\exists u \in \mathbb{Z})(\exists v \in \mathbb{Z})n = ua + vb\}.$$

In other words, $[a, b]$ is the set of all integers that are the sum of a multiple of a and a multiple of b . Equivalently, $[a, b]$ is the set of all integers that are integer linear combinations of a and b .

Prove the following facts:

1. If S is a subgroup of \mathbb{Z} , then $0 \in S$.

2. If S is a subgroup of \mathbb{Z} , then S is closed under the “minus” operation, that is: if a is an arbitrary member of S , it follows that $-a \in S$.
3. If S is a subgroup of \mathbb{Z} , then S is closed under addition, that is: if a, b are arbitrary members of S , it follows that $a + b \in S$.
4. If S is a subgroup of \mathbb{Z} , and $a \in S$, then $[a] \subseteq S$. That is, every multiple ua of a member a of S is in S . (HINT: First prove by induction on n , using Fact 3, that if $n \in \mathbb{N}$ and $a \in S$ then $na \in S$. Then, using this, and Facts 1 and 2, prove that $ua \in S$ also if $u = 0$ or $u < 0$.)
5. If a is an integer, then $[a]$ is a subgroup of \mathbb{Z} .
6. If a, b are integers, then $[a, b]$ is a subgroup of \mathbb{Z} .
7. If a, b are integers, then $[a] \subseteq [b]$ if and only if $b|a$.
8. If S and T are subgroups, then $S \cap T$ is a subgroup. (WARNING: The first thing you will have to prove is that $S \cap T \neq \emptyset$. You know that S and T are nonempty, because they are subgroups. But ***it is not true that the intersection of two nonempty sets is nonempty***. So ***you cannot prove that $S \cap T \neq \emptyset$ by saying “ S is nonempty, and T is nonempty, so $S \cap T$ is nonempty”***. You need a more sophisticated argument.
9. If S is a subgroup of \mathbb{Z} , then
 - (i) there exists a unique nonnegative integer u such that $S = [u]$.
 - (ii) if $S \neq \{0\}$, then the unique nonnegative integer u such that $S = [u]$ satisfies:
 - (a) $u \in \mathbb{N}$,
 - (b) u is the smallest member of $S \cap \mathbb{N}$.

(HINT: Observe that either $S = \{0\}$ or $S \neq \{0\}$, and that if $S = \{0\}$ then $S = [0]$. Prove that if $S \neq \{0\}$ then $S \cap \mathbb{N} \neq \emptyset$. Use the WOP to conclude that $S \cap \mathbb{N}$ has a smallest member. Call this smallest member u , so $u \in \mathbb{N}$. Then prove that $S = [u]$ as follows: the inclusion $[u] \subseteq S$ follows from Fact 4; the inclusion $S \subseteq [u]$ follows from the Division Theorem: let $n \in S$; then write $n = qu + r$ with $0 \leq r < u$; then $r \in S$, because $r = n - qs$; then r must be 0 because if $r > 0$ then $r \in S \cap \mathbb{N}$

and $r < u$, contradicting the fact that u is the smallest member of $S \cap \mathbb{N}$; so $n = qs$ and then $n \in [u]$.)

10. If a, b are integers, and $a \neq 0$ or $b \neq 0$, then the smallest member of $[a, b] \cap \mathbb{N}$ is the greatest common divisor of a and b . (HINT: We know from Fact 6 that $[a, b]$ is a subgroup of \mathbb{Z} , and then Fact 9 tells us that $[a, b] = [g]$ for some $g \in \mathbb{N}$. Show that $a \in [a, b]$ and $b \in [a, b]$, and conclude from this that $g|a$ and $g|b$. Finally, show that if c is any common factor of a and b then $c \leq g$ as follows: show that every member of $[a, b]$ is a multiple of c ; conclude that $[a, b] \subseteq [c]$; infer from this that $g \in [c]$; then g is a multiple of c ; deduce from this that $c \leq g$.)