MATHEMATICS 300 — FALL 2017

Introduction to Mathematical Reasoning

H. J. Sussmann

HOMEWORK ASSIGNMENT NO. 11, DUE ON MONDAY, NOVEMBER 20

This assignment consists of ***four*** *problems.*

Problem 1. *Many students seem to think that "finite" means the same as "bounded". The purpose of this problem is to persuade you that this is not so, by having you prove that some important sets are bounded and infinite.*

In this problem, we use the following terminology and notations:

- If a, b are real numbers, then
  - The open interval from a to b is the set $]a, b[$ given by

$$]a, b[= \{x \in \mathbb{R} : a < x < b\},$$

  - The closed interval from a to b is the set $[a, b]$ given by

$$[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\},$$

Notice that

- If $a > b$ then both sets $]a, b[$ and $[a, b]$ are empty.
- If $a = b$ then $]a, b[$ is empty and $[a, b]$ is the singleton of a, so $[a, b]$ consists of exactly one point.

1. ***Prove*** that if a, b are real numbers such that $a < b$ then the sets $]a, b[$, $[a, b]$ are both bounded and infinite.
2. ***Prove*** that if A is a subset of $\mathbb{Z}$ then A is bounded if and only if A is finite. □

Remark. You have probably seen open intervals before, but the name for them was "(a, b)" rather than "$]a, b[$". I am using "$]a, b[$" here because

1. I think this notation is nicer than "(a, b)".

2. I do not want the interval $]a, b[$ to be confused with the ***ordered pair*** (a, b), so I prefer tno to call the open interval "(a, b)". □

Problem 2. A subset D of $\mathbb{R}$ is said to be dense in $\mathbb{R}$ if every nonempty open interval $]a, b[$ has a nonempty intersection with D. In other words, D is dense in $\mathbb{R}$ if for every pair a, b of real numbers such that $a < b$ there exists a member x of D such that $a < x < b$. (In formal language: D is dense in $\mathbb{R}$ if $(\forall a \in \mathbb{R})(\forall b \in \mathbb{R})\Big(a < b \Longrightarrow (\exists x \in D) a < x < b\Big)$.)

Prove that if D is a dense subset of $\mathbb{R}$ and a, b are real numbers such that $a < b$ then the sets $]a, b[\cap D$, $[a, b] \cap D$ are infinite.

NOTE: *(You don't need to know this to do the problem, but it's good to know.)* Two important examples of subsets of $\mathbb{R}$ that are dense in $\mathbb{R}$ are (a) the set $\mathbb{Q}$ of all rational numbers, (b) the set $\mathbb{I}$ of all irrational numbers. We will prove later that $\mathbb{Q}$ and $\mathbb{I}$ are dense. □

Problem 3. If n is a natural number, and a, b are two integers, we say that a and b are congruent modulo n if $a - b$ is divisible by n.

We write "$a \equiv_n b$" to indicate that a and b are congruent modulo n. (For example, the following sentences are true: $23 \equiv_4 7$, $32 \equiv_{17} 15$, $-5 \equiv_7 9$, $729 \equiv_3 0$, $\sim 33 \equiv_3 2$, $\sim 444 \equiv_2 1$.)

Prove that there are infinitely many primes that are congruent to 3 modulo 4. (That is, prove that the set of all natural numbers n such that $n \equiv_4 3$ and n is prime is an infinite set.)

NOTE: Here are some examples of primes that are congruent to 3 modulo 4: 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103. The result you are asked to prove says that this list can be continued indefinitely, and never stops.)

HINT: Here is a guided list of the steps for your proof.

1. First, you should prove that every integer is congruent modulo 4 to one of the integers 0, 1, 2, 3.

2. Next, you should conclude from the previous step that every odd integer is congruent modulo 4 to 1 or 3.

3. Next, you should prove that every prime number other than 2 is odd.

4. Next, you should conclude from the above that every prime number other than 2 is congruent to 1 or to 3 modulo 4.

5. Then you should show that:

   (a) If a, b, c, d are integers, n is a natural number, and $a \equiv_n b$ and $c \equiv_n d$, then $a + c \equiv_n b + d$ and $ac \equiv_n bd$.

   (b) As a special case of the above result:

      i. The product of two integers that are congruent to 1 modulo 4 is congruent to 1 modulo 4.

      ii. The product of two integers that are congruent to 3 modulo 4 is congruent to 1 modulo 4.

      iii. The product of an integer that is congruent to 3 modulo 4 and an integer that is congruent to 1 modulo 4 is congruent to 3 modulo 4.

   (c) If a natural number n is ≥ 2 and is congruent to 3 modulo 4, then n has a prime factor that is congruent to 3 modulo 4.

6. And now, finally, you should be able to prove the desired conclusion as follows:

   (a) Assume that there is a finite list $\mathbf{p} = (p_j)_{j=1}^r$ of all the primes that are congruent to 3 modulo 4. Let $\mathbf{p}$ be one such list, remove the number 3 from it, and let $\mathbf{q}$ be the resulting list, so $\mathbf{q} = (q_j)_{j=1}^s$ is a list of all the primes that are congruent to 3 modulo 4 and are not equal to 3. (That is: If S is the set of all natural numbers n such that n is prime, $n \neq 3$, and $n \equiv_4 3$, then $\mathbf{q}$ is a list of all the members of S.)

   (b) Let
   $$M = 3 + 4\prod_{j=1}^{s} q_j \,.$$

   (c) Prove that M is not divisible by 3.

   (d) Prove that M has a prime factor u such that $u \equiv_4 3$.

   (e) Prove that u cannot be equal to 3.

   (f) Prove that u cannot be an entry of the list $\mathbf{q}$, and get a contradiction from this.

Problem 4. ***Prove*** that there are infinitely many primes that are congruent to 5 modulo 6. (That is, prove that the set of all natural numbers n such that $n \equiv_6 5$ and n is prime is an infinite set.)

NOTE: Here are some examples of primes that are congruent to 5 modulo 6: 5, 11, 17, 23, 29, 41, 47, 53, 59, 71, 83, 89, 101. The result you are asked to prove says that this list can be continued indefinitely, and never stops.)

HINT: Follow a strategy similar to the one you used for the previous problem.