FALL 2020

OLGA RADKO MATH CIRCLE
ADVANCED 3
DEC 13, 2020

1. Euler's Number and the Least Upper Bound

Problem 1.1. Let $A \subset \mathbb{R}$ be a nonempty subset of real numbers which is bounded from below. Show that there exists a unique real number $b \in \mathbb{R}$ with the following two properties:

(1) For any $a \in A$, $b \leq a$.
(2) If $c \in \mathbb{R}$ has $c \leq a$ for all $a \in A$, then $c \leq b$.

That is, show there is a unique greatest lower bound of A. We call this real number $\inf(A)$.
Hint: You don't need to reprove everything we know about upper bounds.

Problem 1.2. Show that if $A \subset B \subset \mathbb{R}$ are nonempty subsets of real numbers bounded from below, then $\inf(A) \geq \inf(B)$. (If you use any results from the original worksheet, you must reprove them).

Problem 1.3. Let $A, B \subset \mathbb{R}$ be nonempty subsets of real numbers bounded from below. Show $\inf(A + B) = \inf(A) + \inf(B)$. (If you use any results from the original worksheet, you must reprove them).

Problem 1.4. Let $a_1 = 1$ and $a_n = a_{n-1} + \frac{1}{1.5^n} - \frac{1}{n^n}$ for all $n \geq 2$. Prove that the sequence $(a_n)_{n=1}^{\infty}$ converges. You do not need to find what it converges to.

2. Hat Problems

Problem 2.1. Three people are each given a red or a blue hat at random. Each one can see the other people's hats, but not their own. They are told to raise their hands if they see someone wearing a red hat, and a prize is offered to the first person to (correctly) guess their hat color.

All three raise their hands, and several minutes pass. Then somebody guesses "My hat is red", winning the prize. How did they know, and what colors were the other hats?

The following are interactive hat problems. To play one of these problems, please read the problem carefully, agree on a strategy, and then gather a group, and head over to the main breakout room to play.

Problem 2.2. Please gather a group of at least 6.

The instructor will assign each of you a hat color, red, green, or blue, at random. IRL, we might put a real hat on your head with your eyes closed, but today, the instructor will message everyone *except* you your hat color in the chat.

Once everybody is ready, then there are two rounds of guessing. In the first round, the instructor randomly chooses one of you, who guesses their hat color, which is allowed to be incorrect, but they are not told the answer. After two minutes of thinking independently, in the second round, everyone except that first representative must simultaneously guess their hat colors. This second time, you must all get it right.

Problem 2.3. Please gather a group of 3 people.

Each of you will be assigned a red or blue hat, and as before, you will only be told everybody else's hat color.

There is only one round of guessing, you all must guess your hat color, or pass, at once. You win as a group if not everyone passes, and everyone who doesn't pass guesses their hat color correctly.

Because this game is faster, you can play up to 4 times, and you get 1 point for each win.

3. Manifolds

Define a *deformation retraction* from a metric space X to a subspace $A \subset X$ to be a continuous function $H : X \times [0,1] \to X$ with $H(x,0) = x$ for all $x \in X$, $H(x,1) \in A$ for all $x \in X$, and $H(a,t) = a$ for all $a \in A$ and $t \in [0,1]$. We say X *deformation retracts* to A if there is a deformation retraction from X to A.

Problem 3.1. Show $X = \mathbb{R}$ deformation retracts to $A = \{0\} \subset \mathbb{R}$.

Problem 3.2. Show $X = \mathbb{R}^2 \setminus \{(0,0)\}$ deformation retracts to $A = S^1 \subset X$.

Problem 3.3. Show $X = \mathbb{R}^3 \setminus \{(0,0,z) : z \in \mathbb{R}\}$ deformation retracts to $S^1 \times \mathbb{R} \subset X$.

Define a *line* in $\mathbb{RP}^2$ to be the image of a plane through the origin under the map $f : \mathbb{R}^3 \setminus \{0\} \to \mathbb{RP}^2$ given by $f(a,b,c) = [a : b : c]$.

Problem 3.4. Show between any two distinct points $[a : b : c] \in \mathbb{RP}^2$ and $[d : e : f] \in \mathbb{RP}^2$, there is a unique line in $\mathbb{RP}^2$ going through those two points.

Problem 3.5. Show that any two lines in $\mathbb{RP}^2$ intersect at a unique point.

Problem 3.6. Identify the manifold $[0,1] \times [0,1]/\sim$, where $\sim$ is the equivalence relation given by the relations $(x,0) \sim (x,1)$ for all $x \in [0,1]$ and $(0,y) \sim (1,y)$ for all $y \in [0,1]$.

4. Cryptography

Problem 4.1. Calculate $5^{234987299836} \pmod{11}$ without a calculator.

Problem 4.2. My RSA public key is $(n,e) = (493,5)$, and someone sent me an encrypted message:

$$217, 37, 325, 52, 135, 258$$

The message consists of 6 letters, encoded with ASCII, and then encrypted with RSA. However, I forgot my private key. Can you decrypt it for me?

(Hint: `wolframalpha.com` or python will do efficient modular exponentiation. At the former, type “`ab̂ mod c`”, in the latter, type “`mod(a,b,c)`”.)

5. Finite Geometry

Problem 5.1. The game of Pro Set revolves around a deck of cards. Each card has between 1 and 6 colored dots on it, such that for each nonempty subset S of

$$\{\text{red}, \text{orange}, \text{yellow}, \text{green}, \text{blue}, \text{purple}\}$$

, there is exactly one card whose dots are colored with the colors from S. No card has more than one dot of a given color.

A *winning set* of cards in this deck is a nonempty set of cards containing an even number of cards of each color of dot.

- How many cards are there?
- What is the minimum number of cards you need to draw from the deck to guarantee that there is a winning set among those cards?

(Hint: Define the *sum* of a set S of cards to be the card (possibly empty) that has a dot of a given color if and only if there are an odd number of dots of that color in the cards of S. How many cards do you need to draw to find two subsets of the drawn cards that have the same sum?)

6. Miscellaneous

Problem 6.1. Let $\mathbb{F}$ be a field. Show that if $ab = 0$, then $a = 0$ or $b = 0$.

Problem 6.2. Show that there is no field of 10 elements.

Problem 6.3. Let $\mathbb{F}[x]$ denote the set of all polynomials in x with coefficients in the field $\mathbb{F}$. We say $p \in \mathbb{F}[x]$ is *monic* if its leading coefficient is $1 \in \mathbb{F}$. We say a monic nonconstant polynomial $p \in \mathbb{F}[x] \setminus \mathbb{F}$ is irreducible if whenever we write $p = fg$ for $f, g \in \mathbb{F}[x]$, either f or g is constant.

(1) Show $x^2 + 1 \in \mathbb{R}[x]$ is irreducible.
(2) Find an infinite field $\mathbb{F}$ for which $x^2 + 1 \in \mathbb{F}[x]$ is not irreducible.
(3) Find a finite field $\mathbb{F}$ for which $x^2 + 1 \in \mathbb{F}[x]$ is not irreducible.

Problem 6.4. Let $\mathbb{F}_2$ denote the field of two elements. List all irreducible quadratics and all irreducible cubics in $\mathbb{F}_2[x]$. List all irreducible quartics in $\mathbb{F}_2[x]$.

Problem 6.5. Let $\mathbb{F}$ be a field. Set up a graph whose vertices are elements of the field $\mathbb{F}$ and which has undirected edges $\{a, a+1\}$ for any $a \in \mathbb{F}$. Under what conditions on $\mathbb{F}$ is such a graph connected? Under what circumstances is it acyclic?

The following problems are a sequence of problems about p-tuples of integers mod p.

Problem 6.6. Let p be a prime number. Let $[p]$ denote the set $\{0, 1, \ldots, p-1\}$. As usual, let $[p]^p$ denote the set of ordered p-tuples whose elements are in $[p]$. For an element v in $[p]^p$, we denote its terms by $v_0, v_1, ..., v_{p-1}$.

Prove that for all v in $[p]^p$, there exists a unique polynomial (which we call P_v) of one variable, coefficients $\pmod p$, and degree $<= p-1$ such that for all j in $[p]$ (j should be thought of as the index), $P_v[j] \equiv v_j \pmod p$.

Problem 6.7. Define f to be a function from $[p]^p$ to itself that takes an element $v = (v_0, v_1, \ldots, v_{p-1})$ to $(v_{p-1}, v_0, v_1, \ldots, v_{p-2})$.

Prove that for all v in $[p]^p$, P_v and $P_{f(v)}$ are polynomials with the same degree and leading coefficient $\pmod p$.

Problem 6.8. Recall that for $k \geq 0$, f^k is the function f composed with itself k times. f^0 is the identity function. If v_1, v_2 are in $[p]^p$, we define $v_1 + v_2$ to be another element in $[p]^p$ given by adding terms coordinate-wise and taking sums mod p.

This problem is about a recursive sequence in $[p]^p$ which depends on values (v_0, K, J).

Let v_0 be in $[p]^p$. Let K be a sequence of length p^p with elements in p. Let J be a sequence of length p^p with elements in $[p]^p$. (Let's zero-index terms of K and J.)

The recursive sequence $S(v_0, K, J)$ is defined as follows. It has 0^{th} term v_0. $v_1 = f^{k_0}(v_0 + J_0)$. In general, $v_{j+1} = f^{k_j}(v_j + J_j)$.

Prove that there exists a sequence J such that for **any** v_0 and K, the sequence $S(v_0, K, J)$ contains the element $\mathbf{0} := (0, 0, ..., 0)$ in $[p]^p$ at least once. Informally, the state $\mathbf{0}$ is the good state, and we want to choose J to reach the good state at least once.

Hint: Consider the easier problem to find J such that for any v_0 and K where we are guaranteed v_0 has all equal terms), the sequence contains the element $\mathbf{0}$. Next, suppose that we are guaranteed that P_{v_0} has degree 1.