Math Circle - Intro to Proofs 1

Name: Table: November 3, 2019

Problem 0: An integer $x \in \mathbb{Z}$ is called even if $x = 2k$ for some integer $k \in \mathbb{Z}$, and it is called odd if $x = 2k + 1$ for some $k \in \mathbb{Z}$. You may use the fact that every integer is either even or odd (but never both).

a) Show that the product of two odd integers is odd.

b) We say an integer $d \neq 0$ divides an integer $a \in \mathbb{Z}$ if there exists an integer $k \in Z$ with $dk = a$. Let $a \in \mathbb{Z}$. Show that if 5 divides $2a$, then 5 divides a.

c) Prove that for any $n \in \mathbb{Z}$, $5n^2 + 3n + 7$ is odd.

d) Let $a, b, c \in \mathbb{Z}$ with $a^2 + b^2 = c^2$. Show either a is even or b is even.

e) Show every odd integer is the difference of two squares.

You must get your solution to Problem 0 approved by the instructor at your table.

Math Circle - Intro to Proofs 1

Name: Table: November 3, 2019

Problem 1: A real number $r \in \mathbb{R}$ is called *rational* if there exist integers $a, b \in \mathbb{Z}$ with $b \neq 0$ such that $r = a/b$. It is called irrational otherwise.

a) Show $\sqrt{2}$ is irrational.

b) Prove that the product of rational numbers must be rational, while the product of irrational numbers may be rational or irrational. (If you claim a number is irrational, prove it!).

Problem 2: Let $X = \{n \in \mathbb{Z} : n \geq 2\}$. For $k \geq 2$, define $X_k = \{kn : n \in X\}$. What is the set $X \setminus \cup_{k=2}^{\infty} X_k$? Prove your claim.

Problem 3: For a set X, define the *diagonal* of the set to be the subset of $X \times X$ given by $\Delta(X) = \{(i,i) \in X \times X : i \in X\}$.

A (simple undirected) graph is an ordered pair $G = (V, E)$, where V is a set, and $E \subset V \times V$ is a subset with $(i,j) \in E \iff (j,i) \in E$, and $E \cap \Delta(V) = \emptyset$. The elements of V are called vertices, and the elements of E are called edges.

a) (Conceptual) Explain what the conditions on the set E mean.

b) (Conceptual) The *degree* $\delta(i)$ of a vertex $i \in V$ is, intuitively, the number of edges touching that vertex. Write down a formal definition of $\delta(i)$ by writing it as the size of a particular subset of E. Use set-builder notation similar to the definitions seen above. Recall that if X is a set, $|X|$ denotes its cardinality (size).

c) There are 9 people at a party. Show that it is impossible for each of them to be friends with exactly 3 other people at the party (assuming friendship is always mutual).

Problem 4: Recall a function $f : X \to Y$ is injective if $f(x) = f(y)$ implies $x = y$. A function $f : X \to Y$ is surjective if for each $y \in Y$, there exists an $x \in X$ with $f(x) = y$.

Let A, B, C be sets, and let $f : A \to B$ and $g : B \to C$ be functions. Define $h = g \circ f$.

a) Show that if h is injective, then f is injective. Show that g may not necessarily be injective.

b) Show that if h is surjective, then g is surjective. Show that f may not necessarily be surjective.

Problem 5: Let $X = \{1, 2, 3, ..., n\}$ for some integer $n \geq 2$. Let k be an integer with $1 \leq k \leq n-1$. Let $E = \{Y \subset X : |Y| = k\}$. Let $E_1 = \{Y \in E : 1 \in Y\}$ and $E_2 = \{Y \in E : 1 \notin Y\}$.

a) Show $\{E_1, E_2\}$ is a partition[1] of E. That is, show $\emptyset \neq E_1 \subset E$, $\emptyset \neq E_2 \subset E$, $E_1 \cup E_2 = E$ and $E_1 \cap E_2 = \emptyset$.

b) Compute $|E_1|$, $|E_2|$, and $|E|$. You may use the fact that the number of subsets of size k of a set of size n is precisely $\binom{n}{k}$. Recall

$$\binom{n}{k} = \frac{n!}{(n-k)! \cdot k!}$$

c) Conclude for any $n \geq 2$ and $1 \leq k \leq n-1$, $\binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k}$.

d) For $t \in \mathbb{N}$, show $\binom{2t}{t}$ is even.

[1] Let X be a nonempty set. Let $\mathcal{P}(X)$ be its power set (the set of all subsets of X). A *partition* of X is a subset $S \subset \mathcal{P}(X)$ such that $\bigcup_{A \in S} A = X$ and for all $A, B \in S$, if $A \neq B$, then $A \cap B = \emptyset$. To avoid redundancies, we also insist every element of S is nonempty.

Problem 6: For this problem, you may need the division algorithm[2] and the well-ordering principle[3].

Let $x, y \in \mathbb{N}$ be natural numbers. Consider the set $S = \{ax + by : a, b \in \mathbb{Z}, ax + by > 0\}$.

a) Show S has a least element. Hereafter, we denote this as the element $d \in S$.

b) Let $z = \gcd(x, y)$. Show z divides d.

c) Show d divides x and d divides y.

d) Prove or disprove: $\gcd(x, y) \in S$.

[2] **Theorem** (Division Algorithm): Let $a, b \in \mathbb{Z}$ be integers with $a > 0$. Then there exist unique integers $q, r \in \mathbb{Z}$ with $b = aq + r$ and $0 \leq r < a$.

[3] The well-ordering principle states that every nonempty subset of the natural numbers has a least element.

Problem 7: Revisit Problem 4 for the definition of injective and surjective functions.

a) Let $f : X \to Y$ be an injective function. Show that for any two functions $g : Z \to X$ and $h : Z \to X$, if $f \circ g = f \circ h$ as functions from Z to Y, i.e. they agree on every input $z \in Z$, then $g = h$ as functions from Z to X. (This is a one line proof, so try to sort out what's happening).

b) Let $f : X \to Y$ be a surjective function. Show that for any two functions $g : Y \to W$ and $h : Y \to W$, if $g \circ f = h \circ f$ as functions, then $g = h$ as functions.

c) * Let $f : X \to Y$ be a function such that for any set Z and any two functions $g : Z \to X$ and $h : Z \to X$, if $f \circ g = f \circ h$, then $g = h$. Show that f is injective.

d) * Let $f : X \to Y$ be a function such that for any set W and any two functions $g : Y \to W$ and $h : Y \to W$, if $g \circ f = h \circ f$, then $g = h$. Show f is surjective.

Problem 8: In this problem we prove the binomial theorem: for real numbers a, b and natural number $n \geq 0$, we have

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

To prove this result, we first let $a, b \in \mathbb{R}$ be arbitrary.

a) Verify the formula works for $n = 0$. You should probably also try out $n = 1, 2, 3$ just to get a sense of what is going on.

b) Let $N \in \mathbb{N}$ be a fixed natural number. Suppose we know for that specific value, $n = N$, that

$$(a+b)^N = \sum_{k=0}^{N} \binom{N}{k} a^k b^{N-k}$$

Multiply both sides of this equation by $a + b$ and simplify, to show

$$(a+b)^{N+1} = \sum_{k=0}^{N+1} \binom{N+1}{k} a^k b^{N+1-k}$$

i.e. that the formula above works for $n = N + 1$.

c) Conclude the formula works for all natural numbers $n \geq 0$. Since $a, b \in \mathbb{R}$ were arbitrary, we conclude it works for all $a, b \in \mathbb{R}$ and all $n \geq 0$.

Problem 9: A *relation* on a set X is a subset $R \subset X \times X$. R is called *reflexive* if $(x, x) \in R$ for each $x \in X$. It is called *symmetric* if $(x, y) \in R \Rightarrow (y, x) \in R$. It is *transitive* if $(x, y), (y, z) \in R \Rightarrow (x, z) \in R$. A relation that is reflexive, symmetric and transitive is called an *equivalence relation*. The *equivalence class* of an element $x \in X$ is the set $[x] = \{y \in X : (x, y) \in R\}$.

Let R be an equivalence relation on a nonempty set X. Show the collection of equivalence classes $\{[x] : x \in X\}$ (as defined above) is a partition of X. (Recall a partition of X is a collection of nonempty subsets of X which are pairwise disjoint and whose union is all of X.)

Problem 10: Revisit problem 3 for the definition of an undirected graph, and the degree of a vertex.

Let $G = (V, E)$ be an undirected graph. A *path* in G is a sequence of vertices $v_0, v_1, ..., v_n \in V$ (for some $n \geq 0$) such that $(v_i, v_{i+1}) \in E$ for each $i = 0, ..., n-1$. Such a path is called a path from v_0 to v_n.

A graph is *connected* if for any $v, w \in V$, we have a path from v to w.

a) Let R be a relation on V given as follows: $(v, w) \in R$ if and only if there is a path from v to w in G. Show R is an equivalence relation. Its equivalence classes are called the connected components of G. Do you see why?

b) Let G be a graph with 10 vertices (i.e. $|V| = 10$), such that each vertex has degree exactly 5. Consider the following proofs that G is connected. Which of these are correct, and which are incorrect?

i) Suppose G is not connected. Let's group the vertices into two groups of 5 vertices each. Draw edges from each vertex to other vertices within its group. Now every vertex has degree 4. We need every vertex to have degree 5, but on the other hand, adding even one more edge makes the graph connected. So we cannot simultaneously have all degrees 5 while also keeping the graph disconnected. By contradiction, the graph must be connected.

ii) Suppose G is not connected. Let $v, w \in V$ be two arbitrary vertices. Since v has degree 5, it is connected to five vertices v_1, v_2, v_3, v_4, v_5. Since w has degree 5, it is connected to five vertices, w_1, w_2, w_3, w_4, w_5. In total, this is 12 vertices, but we only have 10. By contradiction, we must have G is connected.

iii) Let $v, w \in V$ be arbitrary. If $v = w$, there is a trivial path via $v_0 = v$.

Suppose $v \neq w$. If they have an edge between them, we have a path from v to w via the sequence of vertices $v_0 = v, v_1 = w$.

Suppose $v \neq w$ and there is not an edge between them. Since v has degree 5, it is connected to five (distinct) vertices $v_1, ..., v_5$. Since w has degree 5, it is connected to five (distinct) vertices $w_1, ..., w_5$. Since there are in total 10 vertices, we must have a repeat in the list $v, w, v_1, ..., v_5, w_1, ..., w_5$. Since $v \neq w$, those cannot be the repeats. Since there is no edge from v to w, w cannot appear on the list $v_1, ..., v_5$. Similarly, v cannot appear in the list $w_1, ..., w_5$. There also can't be a repeat with $v_i = v_j$ for some $i \neq j$, or $w_i = w_j$ for $i \neq j$. Thus, we must have $v_i = w_j$ for some i, j. But then we have a path $v_0 = v, v_1 = w_j, v_2 = w$, since $(v_0, w_j) = (v_0, v_i) \in E$, and $(w_j, w) \in E$.

Note $v, w \in V$ were arbitrary, and we've shown there is a path between them in all cases above. Thus, G is connected. (In fact, we've shown there is a path of length at most 2 between any two vertices of G).

iv) Let $v, w \in V$ be arbitrary. We show there is a path from v to w. If $v = w$ there is nothing to show. If there is an edge from v to w, there is again nothing to show. Now, other than v and w, there are 8 vertices left. v must have edges to 5 of them, and w must have edges to 5 of them. Thus, by the pigeonhole principle, there must be some vertex of the remaining 8, call it x, which has an edge to both v and w. Then $v_0 = v, v_1 = x, v_2 = w$ is a path in G. Since $v, w \in V$ were arbitrary, we conclude G is connected.

v) Note $v \in V$ is connected to 5 other vertices. Thus, its connected component has size at least 6 vertices. Since v was arbitrary, it must be that any connected component has size at least 6. On the other hand, the sum of the number of vertices in each connected component is 10.

More formally, let $C_1, ..., C_k \subset V$ be the connected components. We have $|C_1| + ... + |C_k| = 10$, but also, each $|C_i| \geq 6$. So $10 = |C_1| + ... + |C_k| \geq 6 + ... + 6 = 6k$. So $6k \leq 10$, and $k \leq 10/6 < 2$. So the number of connected components is at least 1 and is strictly less than 2. Since it is an integer, it must be precisely $k = 1$. Thus, the graph is connected.

vi) We prove by induction on n that for any choice $v_1, v_2, \ldots, v_n$ of n distinct vertices of G, all $v_1, v_2, \ldots, v_n$ lie in the same connected component of G. Once this is established, the case $n = 10$ gives the desired result. (Note that for $n > 10$, this statement is vacuously true, since there are no choices of n distinct vertices about which we are making a claim. This is analogous to the fact that every unicycling elephant enrolled in LAMC knows a proof of the Riemann Hypothesis in ZFC and will show it to you if you give it candy.)

Base case $n = 1$: In this case, there is only one vertex, so it certainly lies in the same connected component as itself.

Inductive step: Supposing the result is known for any choice of n distinct vertices, we show that the same is true for any choice of $n+1$ distinct vertices. If $n+1 > 10$, this is vacuously true of any choice of $n+1$ distinct vertices since there are no such choices; otherwise fix any distinct vertices $v_1, v_2, \ldots, v_{n+1}$. Considering the set $v_1, v_2, \ldots, v_n$, the inductive hypothesis gives that $v_1, v_2, \ldots, v_n$ all lie in the same connected component of G. In particular, there is some path in G (which may use vertices outside of our chosen ones!) from v_1 to v_n. On the other hand, considering the n distinct vertices $v_2, v_3, \ldots, v_n, v_{n+1}$, the inductive hypothesis tells us that there is similarly a path from v_n to v_{n+1}. Combining the path from v_1 to v_n with the path from v_n to v_{n+1} gives a path from v_1 to v_{n+1}. Of course, since the labelling $v_1, v_2, \ldots, v_{n+1}$ was arbitrary, given any two distinct vertices in that set, we may arrange for one of them to labeled v_1 and the other v_{n+1}, so this shows that any two vertices in $v_1, v_2, \ldots, v_{n+1}$ are connected by a path in G and hence lie in the same connected component.

Challenge Topic - Group Actions

A binary operation $*$ on a set X is a function $*: X \times X \to X$. For $*(a,b)$, we write $a*b$. A binary operation is associative if $*(*(a,b),c) = *(a,*(b,c))$, i.e. $(a*b)*c = a*(b*c)$.

An identity element $e \in X$ is an element such that for each $x \in X$, we have $e*x = x*e = x$. An element $y \in X$ is called an inverse of $x \in X$ if $y*x = x*y$ is an identity element.

A **group** is a set G along with a binary operation $*$ such that $*$ is associative, G has an identity element, and each $g \in G$ has an inverse. We write $(G,*)$ or simply G for the group.

1. Let $(G,*)$ be a group. Show that if $e, e' \in G$ are identity elements, then $e = e'$. Show if $y, y' \in X$ are inverses of $x \in X$, then $y = y'$.
2. Let X be a set, and define $Sym(X) = \{f : X \to X | f \text{ is a bijection}\}$. Show $Sym(X)$ with the operation of function composition is a group. For $|X|$ finite of size n, what is $|Sym(X)|$?
3. Let G and H be groups. A *group homomorphism* is a function $f : G \to H$ such that $f(g*h) = f(g)*f(h)$. Show $f(e_G) = e_H$ (identity maps to identity).
4. An *action* of a group G on a set X is a homomorphism $\phi : G \to Sym(X)$. For $g \in G, x \in X$, we write $g.x$ for $\phi(g)(x)$.

   The *stabilizer* of $x \in X$ under a group action is written as $G_x = \{g \in G : g.x = x\} \subset G$. Show G_x is a subgroup of G. (A subset $H \subset G$ is a *subgroup* if the group operation on G can be restricted to an operation on H, and H is a group with respect to this operation.)
5. Let $H \subset G$ be a subgroup and $g \in G$ an element. Define the (left) *coset* gH as $gH = \{gh : h \in H\}$. Set up an equivalence relation[4] on G whose equivalence classes are precisely the cosets, and conclude the cosets partition G. We write $G/H = \{gH : g \in G\}$ as the set of cosets.
6. The *orbit* of an element $x \in X$ is written as $G.x = \{g.x \in X | g \in G\}$. Prove the *Orbit-Stabilizer Theorem*: if G is a finite group and X is a finite set, then

   $$\frac{|G|}{|G_x|} = |G.x|$$

   for each $x \in X$.

Hereafter, we assume $|G|$ and $|X|$ are finite.

7. Show that the orbits of a group action of G on set X partition X. Show that the number of orbits is precisely $\frac{1}{|G|}\sum_{g\in G} |X^g|$, where

   $$X^g = \{x \in X | g.x = x\}$$
8. An action of G on a set X is called *transitive* if $G.x = X$ for some $x \in X$. Show that this implies $G.y = X$ for any $y \in X$.
9. For $H \subset G$ a subgroup, G acts naturally on G/H via $k.(gH) = (kg)H$, for $k, g \in G$. Show that this is well-defined (i.e. if $gH = g'H$, then $(kg)H = (kg')H$). Show that this action is transitive.
10. Show that if G acts transitively on a set X, we may find a subgroup $H \subset G$ and a bijection $f : X \to G/H$ with $f(g.x) = g.f(x)$ for each $g \in G$ and $x \in X$.

[4] A *relation* on a set X is a subset $R \subset X \times X$. R is called *reflexive* if $(x,x) \in R$ for each $x \in X$. It is called *symmetric* if $(x,y) \in R \Rightarrow (y,x) \in R$. It is *transitive* if $(x,y),(y,z) \in R \Rightarrow (x,z) \in R$. A relation that is reflexive, symmetric and transitive is called an *equivalence relation*. The *equivalence class* of an element $x \in X$ is the set $[x] = \{y \in X : (x,y) \in R\}$.

Exercise: Show the collection of equivalence classes $\{[x] : x \in X\}$ (as defined above) is a partition of X.