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.

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.

Problem 2: Let $X = \{n \in \mathbb{Z} : n \geq 2\}$. For $k \in X$, define $X_k = \{kn : n \in \mathbb{N}\}$. 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 $E_1 \subset E$, $E_2 \subset E$, $E_1 \cup E_2 = E$ 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 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 $A \cap B = \emptyset$ for all $A, B \in S$ with $A \neq B$.

Problem 6: The well-ordering principle states that every nonempty subset of the natural numbers has a least element.

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: $\gcd(x, y) \in S$.

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 that the group operation on G can be restricted to G_x, and that G_x is itself a group with this operation. (Under such conditions, we say G_x is a *subgroup* of G).

5. 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.

6. 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

$$X^g = \{x \in X | g.x = x\}$$

7. 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 $y \in X$.

8. For $H \subset G$ a subgroup and $g \in G$ an element, we define the (left) *coset* gH as $gH = \{gh : h \in H\}$. Set up an equivalence relation[2] 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.

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 $x \in X$.

---

[2]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.