Middle East Technical University
Computer Engineering Department

CENG 223
Fall 2024 - Homework 3

1 Questions

Q1) Divisibility and Elementary Number Theorem

1. Prove that for any positive integers $k, n \in \mathbb{N}_0$,

$$\sum_{j=1}^{n} j(j+1)\dots(j+k-1) = \frac{n(n+1)\dots(n+k)}{k+1}$$

2. Prove that for a prime p, a positive integer x not divisible by p, and the smallest positive integer y such that $x^y \equiv 1 \pmod{p}$, $y \mid (p-1)$.
3. Prove that for any integer $n \in \mathbb{N}$,

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

Hint: Use mathematical induction and consider binomial expansion techniques in your proof.

Q2) Inductive Proofs and Fundamental Theorems

Let $n, k \in \mathbb{N}$ and $\mathcal{X}$ be the set of n numbers (variables), i.e. $\mathcal{X} = \{x_1, x_2, \dots, x_n\}$. A **power sum symmetric polynomial** $p_k \in \mathbb{R}[\mathcal{X}]$ is defined as:

$$p_k(x_1, x_2, \dots, x_n) = \begin{cases} n & : k = 0 \\ \sum_{j=1}^{n} x_j^k & k \in \mathbb{N}_0 \end{cases},$$

An **elementary symmetric polynomial** $e_k \in \mathbb{R}[\mathcal{X}]$, is the sum of all products of k distinct variables chosen from $x_1, x_2, \dots, x_n$:

$$e_k(x_1, x_2, \dots, x_n) = \begin{cases} 1 & : k = 0 \\ \sum\limits_{1 \le i_1 < i_2 < \dots < i_k \le n} x_{i_1} x_{i_2} \cdots x_{i_k} & : 1 \le k \le n \\ 0 & : n < k \end{cases},$$

For example:

$$e_1(x_1, x_2, \dots, x_n) = x_1 + x_2 + \dots + x_n, \qquad e_2(x_1, x_2, \dots, x_n) = \sum_{1 \le i < j \le n} x_i x_j,$$

and so on. A **symmetric polynomial** $f \in \mathbb{R}[\mathcal{X}]$ is a polynomial that remains invariant under any permutation of its variables. That is, for any bijection (or permutation) $\sigma : \{1, \dots, n\} \to \{1 \dots, n\}$ of the indices $1, 2, \dots, n$, $f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) = f(x_1, x_2, \dots, x_n)$. For example, $f(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2$ is symmetric, as swapping any pair of x_i's does not change f.

1. (*ungraded*) Prove that every integer greater than 1 can be represented as a product of prime numbers, up to the order of the factors.

   Hint: Fundamental theorem of arithmetics.

2. Prove the Fundamental Theorem of Arithmetic using mathematical induction.

   Fundamental Theorem Statement: Every integer greater than 1 can be **uniquely** represented as a product of prime numbers, up to the order of the factors.

3. Prove that for any positive integer $k \in \mathbb{N}_0$, Newton's identities (Newton-Girard formulas) relate the elementary symmetric polynomials e_i to the power sums of variables p_k as follows:

$$ke_k = \sum_{i=1}^{k} (-1)^{i-1} e_{k-i} p_i \quad : 1 \le k \le n$$

$$0 = \sum_{i=k-n}^{k} (-1)^{i-1} e_{k-i} p_i \quad : 1 \le n < k$$

   where $p_k = \sum_{j=1}^{n} x_j^k$ is the k-th power sum symmetric polynomial and $e_k(x_1, x_2, \dots, x_n) = \sum_{1 \le i_1 < i_2 < \dots < i_k \le n} x_{i_1} x_{i_2} \cdots x_{i_k}$ is the k-th elementary symmetric polynomial.

4. Prove the fundamental theorem of symmetric polynomials (without uniqueness).

   Funamental Theorem Statement: For any symmetric polynomial $f(x_1, x_2, \dots, x_n) \in \mathbb{R}[\mathcal{X}]$, there exists a polynomial $F \in \mathbb{R}[\mathcal{X}]$ such that $f(x_1, x_2, \dots, x_n) = F(e_1, e_2, \dots, e_n)$, where e_i are the elementary symmetric polynomials, and $f(x_1, x_2, \dots, x_n)$ is defined as a symmetric polynomial, i.e. a polynomial invarian under permutations of $x_1, x_2, \dots, x_n$.

Q3) Multisets and Combinatorial Applications

A **multiset** (S, f) is a **set** with repetitions allowed, where S is a **set** and $f : S \to \mathbb{N}_0$ assigns a non-negative integer multiplicity to each element in S. We often denote it as $\{s_1^{f(s_1)}, \ldots, s_n^{f(s_n)}\}$. For example, $\{1, 1, 2, 4, 4, 4\}$ is a 4-multiset (of size 6) on the set $\{1, 2, 3, 4\}$ and is denoted as $\{1^2, 2^1, 3^0, 4^3\}$.

1. Show that the number of c-multisets of size n, denoted as $\mathcal{M}(c, n)$, is given by $\binom{c+n-1}{n}$ for all $c, n \in \mathbb{N}_0$.
2. How many solutions does the equation $x_1 + \cdots + x_{12} = 13^2$ have, where $x_1, x_2, \ldots, x_{12} \in \mathbb{N}_0$?
   Hint: Think of distributing 13^2 identical objects into 12 distinct bins.
3. How many seven-digit positive integers contain the digit 9 at least once and are divisible by 3?
   Recall: a number is divisible by 3 if the sum of its digits is divisible by 3.

Q4) Symmetries of a Regular n-gon

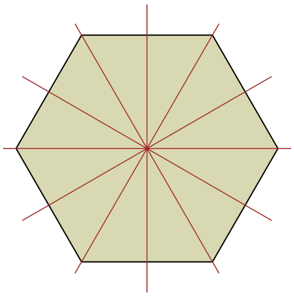

Figure 1: The six axes of reflection of a regular hexagon (6-gon).

Consider a regular n-gon (a polygon with n sides and n vertices) centered at the origin on the 2D plane. Let V be the set of its vertices. Let D_n be the set of all bijective functions from V to V that map the n-gon onto itself, while preserving its geometry[1].

1. Find the cardinality of the set D_n. Is the set finite? If so, determine the number of elements in D_n. If not, show that D_n is an infinite set.
2. Assume the following:
   - The function $r : V \to V$ corresponds to a rotation symmetry of the n-gon by an angle of $\frac{2\pi}{n}$ radians (i.e., a rotation that maps each vertex to the next vertex in a clockwise direction).
   - The function $s : V \to V$ corresponds to a reflection symmetry of the n-gon about an axis of symmetry (for example, a line passing through a vertex and the center of the n-gon).

   Consider the set S generated by r and s under function composition, following these rules:

   (a) **Closure**: For any a, b in S, the composition $a \circ b$ is also in S.

   (b) **Order of Rotation**: For the rotation r, $r^n = e$, where e is the identity function (no rotation or reflection).

   (c) **Order of Reflection**: For the reflection s, $s^2 = e$.

   (d) **Conjugation Relation**: Using (2) and (3), $s \circ r \circ s^{-1} = r^{-1}$, where $\circ$ is function composition.

   Show that the set S, generated by r and s with the above properties, is isomorphic to D_n.
3. Partititon D_n into equivalence (or self-conjugacy) classes such that the total number of equivalence classes are minimum.
   Definition: let $a \in D_n$, the equivalence class of element a is $[a] = \{aba^{-1} \in D_n : b \in D_n\}$.

Q5) Rubik's Cube Twists and Their Properties

Alice labels each of the movable cubies of the Rubik's Cube with numbers from 1 to 48 (excluding the fixed center cubies). Let $\mathbb{Z}_{48} = \{1, 2, 3, \ldots, 48\}$ represent all the numbers assigned to the cubies. She defines a bijective function $f : \mathbb{Z}_{48} \to \mathbb{Z}_{48}$ (i.e., a permutation) such that $f(i) = j$ means that after applying the 'clockwise-front' move, the cubie that was originally at position i moves to position j. In other words, $f(i) = j$ tells us where each cubie ends up after rotating the front face of the cube clockwise by 90 degrees.

More formally, let $\mathcal{R}$ be the set of all possible finite twists (moves) of a Rubik's Cube, each of which can be represented as a bijective function (permutation) on $\mathbb{Z}_{48}$. The set $\mathcal{R}$ can be generated recursively (via function composition) from the one-step basic moves (twists) f, b, r, l, u, d, representing rotations of any side of the cube by $\frac{\pi}{2}$ (90 degrees) in the clockwise direction.

Each basic move can be thought of as a function that rearranges the cubies:

- f: Rotation of the front face clockwise.
- b: Rotation of the back face clockwise.
- r: Rotation of the right face clockwise.

[1] preserving geometry means that it preserve neighboring structure of vertices of the n-gon.

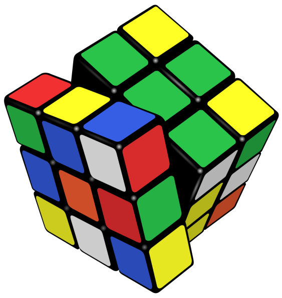

Figure 2: An illustration of an unsolved Rubik's Cube

- l: Rotation of the left face clockwise.
- u: Rotation of the up face clockwise.
- d: Rotation of the down face clockwise.

By combining these basic moves through function composition (performing one move after another), we can create more complex sequences of moves. These sequences form the set $\mathcal{R}$, encompassing all possible permutations of the cubies achievable through twists of the Rubik's Cube. Every element a in $\mathcal{R}$ can be generated via performing finitely many basic moves one after another, e.g. $a = fbr^2u$.

1. Find the cardinality of the set $\mathcal{R}$ of all possible basic twists of the Rubik's Cube. Leave the result as multiplication of permutations, combinations, and factorials. Also justify briefly your answer.
2. Determine the minimal number of twists required to solve the Rubik's Cube from any scrambled state.
   Hint: Use the Pigeonhole Principle in your reasoning.
3. Let the order of an element f be the smallest positive integer m such that $f^m = e$, where e is the identity element (no twist). Show that there exists a finite m for every element f in $\mathcal{R}$.
4. (*ungraded*) Use induction to show that every element f in $\mathcal{R}$ changes an even number of cubies.

2 Submission Guidelines

- **Solution**: To complete this homework:
  - There are 3 graded problems in each question, you may skip "*ungraded*" problems.
  - There are 4 graded questions, you can also skip either Q4 or Q5 (but not both).

  meaning that, solving 3×4 problem is enough.
- **Format**: Submit your solutions in a well-organized document. Clearly indicate each question and its corresponding proof to facilitate easy navigation and review.
- **Deadline**: 15 December 2024 (Sunday)
- **Assessment Criteria**:
  - **Correctness**: Accuracy and validity of your proofs.
  - **Logical Flow and Structure**: Clear and logical progression of ideas.
  - **Mathematical Rigor and Notation**: Proper use of mathematical language and symbols.
  - **Completeness**: Thoroughly addressing all parts of each question.

3 Additional Notes

- **Assumptions**: If you make any assumptions in your reasoning, state them clearly within your proofs.
- **Diagrams and Illustrations**: Feel free to include diagrams or illustrations where they can aid in the clarity and understanding of your explanations.
- **References**: You may use any theorems or results discussed in class or in the textbook, provided you cite them appropriately.