CSC3001: Discrete Mathematics

Assignment 2

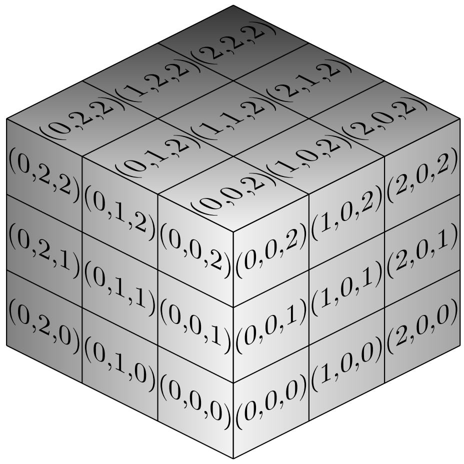
Instructions:

1. Print out this question paper (**two-sided**) and write down your full working on the blank area.
2. You can have discussions with your classmates. However, make sure all the solutions you submit are your own work. Any plagirism will be given **ZERO** mark.
3. Submission of this assignment should **NOT** be later than **5pm on 8th of November**.
4. Before your submission, please **make a softcopy** of your work for further discussion in a tutorial.
5. After making your softcopy, submit your assignment to the dropbox located on the 4th floor in Chengdao Building.

Student Number: ____________________ **Name:** _______________

1. (*20 points*) Let p be an odd prime. Prove that there are exactly $\frac{p-1}{2}$ integers $a \in \{1, \ldots, p-1\}$ such that $x^2 \equiv a \pmod{p}$ for some x.

2. (*20 points*) Suppose that n^3 unit cubes are stacked into a large $n \times n \times n$ cube. Let $x, y, z \in \mathbb{Z}_n$ and label each unit cube by (x, y, z) with respect to its location (see the picture for $n = 3$).



The unit cubes (x, y, z) and (x', y', z') are adjacent if one of the following conditions holds:

- $x' - x \equiv \pm 1 \pmod{n}$ and $y' = y, z' = z$; or
- $|y' - y| \equiv 1 \pmod{n}$ and $x' = x, z' = z$; or
- $|z' - z| \equiv 1 \pmod{n}$ and $x' = x, y' = y$.

For each $n \in \mathbb{Z}^+$, provide an ordering of all the unit cubes satisfying the following:

- every two consecutive cubes are adjacent;
- the last cube and the first cube in the list are adjacent.

(**Note:** You may draw pictures to demonstrate your idea.)

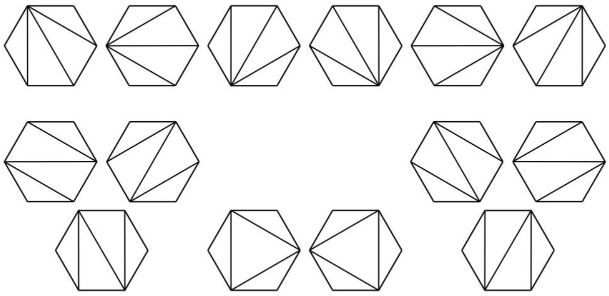
3. (*20 points*) Let $n \in \mathbb{N}$ be with $n \geq 2$. Let $k \in \{1, 2, \ldots, n-1\}$ be a fixed number such that $\mathsf{gcd}(k, n) = 1$. Given the balls labeled by $1, 2, \ldots, n-1$, we try to color each ball black or white such that

(1) i and $n - i$ are of the same color;

(2) for each $i \neq k$, we have i and $|i - k|$ are of the same color.

Prove that all the balls are of the same color.

4. (*20 points*) Let T_n denote the number of different ways that a convex polygon with $n+2$ sides can be cut into triangles by connecting vertices with non-crossing line segments. (For example, $T_n = 14$ for $n = 4$ as shown below)



Find the recurrence relation of T_n and hence find the closed form of T_n using generating functions.

5. (*20 points*) Consider the linear congruence

$$17x \equiv 9 \pmod{276}$$

(a) Show that this congruence has a unique solution.

(b) Show that the given congruence and the following system have the same solution.

$$\begin{cases} x \equiv 0 \pmod{3} \\ x \equiv 1 \pmod{4} \\ 17x \equiv 9 \pmod{23} \end{cases}$$

(c) Solve the original congruence without assistance of calculator.

6. (*10 points*) [**bonus question**] *"A computer is to a number theorist, like a telescope is to an astronomer. It would be a shame to teach an astronomy class without touching a telescope; likewise, it would be a shame to teach this class without telling you how to look at the integers through the lens of a computer."* - **William Stein, Number Theorist**

Consider a *perfect number*, defined as a positive integer n such that it is equal to the sum of all its positive divisors, excluding n itself. Denoting the sum of positive divisors of n by $\sigma(n)$, then a perfect number has the property that

$$\sigma(n) - n = n$$

Denoting the k-th perfect number by P_k, we have

$$P_1 = 6, \; P_2 = 28, \; P_3 = 496, \; P_4 = 8128$$

Based on the above patterns, there were some early conjectures regarding perfect numbers:

A. the n-th perfect number contains exactly n digits; and

B. the even perfect numbers end, alternately, in 6 and 8; and

C. there is no odd perfect number.

By means of a computer program, disprove the first two of these conjectures by finding and examining the fifth and the sixth perfect number. The third conjecture remains an open problem.

(**Note:** You will need to provide pseudocodes, and you may just concentrate on disproving (A) by actually running your program.)