

MATH6005 Semester 2, 2024 Assignment 2

There are four questions. You may find some questions more difficult/time-consuming than others, but nevertheless each question is worth the same, 5 marks. Your total score out of 20 marks will determine 10% of your final grade. The assignment is due by 16:00 on the Monday of Teaching Week 9 (30th of September). Submission instructions will be available on Wattle at least one week before the due time. Late submissions are not accepted without an extension. You are strongly advised to submit your assignment well before the due time to allow for unforeseen circumstances.

You should write in complete (English and mathematical) sentences.

Your solutions should be submitted in the form of a .pdf document, with your solution to each new problem starting on a new page. You may typeset your solutions, but you do not need to. More information about how to prepare and submit your solutions will be provided on the class wattle page.

You may discuss your approach to various problems with other students, but you must write your own solutions. For example, you may discuss ideas for how to solve a problem with a classmate, but then you should not keep notes of the discussion, and should write from a blank page to a complete solution on your own. You may NOT use AI in preparing your solutions. It is likely to be unhelpful. To ensure you have followed these instructions, you must include a collaboration statement as part of your assignment submission. Failure to include such a statement may be penalised in the grading scheme. Further Instructions will be available on Wattle.

You will submit your assignments through Gradescope. Instructions will be available on Wattle.

Question 1

A Consider the statement:

“The product of any even integer and any odd integer is even.”

I While searching online you find the following attempt at a proof of the statement:

“Suppose that m is an even integer and n is an odd integer. Since m is even and n is odd, there exists an integer k such that $m = 2k$ and $n = 2k + 1$. Thus

$$mn = 2k(2k + 1) = 4k^2 + 2k = 2(2k^2 + k) = 2q,$$

where $q = 2k^2 + k$ is an integer. By definition of even, mn is even.”

Explain why the proof is incorrect.

II Give a correct proof of the statement.

B Use mathematical induction to prove that for every integer $n \geq 3$,

$$\sum_{k=3}^n 4^k = \frac{4(4^n - 16)}{3}.$$

C Consider the following sequence of numbers:

$$S = (3, 1, 4, 1, 5, 9, 2, 6)$$

I Trace the Selection Sort Algorithm on S with ordering rule “ \geq ” and count how many comparisons were made. Note that you **DO** need to introduce an indexing set to trace this algorithm.

An example of how to trace is on Slide 12 of Lecture 12.

II Trace the Merge Sort Algorithm on S with ordering rule “ \geq ” and count how many comparisons were made. Note that you **DO NOT** need to introduce an indexing set to trace this algorithm.

An example of how to trace is on Slide 8 of Lecture 13.

III Without tracing the algorithm, how many comparisons are required to complete the Selection Sort Algorithm on S with ordering rule “ \leq ”. Explain your answer.

IV Explain why we would need to trace the Merge Sort Algorithm on S with ordering rule “ \leq ” if we wanted to count the number of comparisons it required. Note that you **DO NOT** need to trace the algorithm or calculate the number of comparisons.

Question 2

A In this question we will consider two different functions with domain and codomain \mathbb{Q}^3 .

I Let F be the function defined by:

$$\begin{aligned} F: \mathbb{Q}^3 &\rightarrow \mathbb{Q}^3 \\ (x, y, z) &\mapsto (4x - 3y + 2z, 3y, x + y + z). \end{aligned}$$

Is F linear? If so prove it, otherwise explain why it is not. Note that you may assume that F is a function.

II Let f be the function defined by:

$$\begin{aligned} f: \mathbb{Q}^3 &\rightarrow \mathbb{Q}^3 \\ (x, y, z) &\mapsto (4x - 3y + 2z, 3y + 1, x + y). \end{aligned}$$

Is f linear? If so prove it, otherwise explain why it is not. Note that you may assume that f is a function.

B Let $(s_n)_{n \in \mathbb{N}} \subseteq \mathbb{Q}^2$, where $s_n = (a_n, b_n)$ is defined implicitly by:

$$s_1 = (1, 0) \text{ and } \forall n \in \mathbb{N} \quad \begin{cases} a_{n+1} = 77a_n - 90b_n, \\ b_{n+1} = 60a_n - 70b_n. \end{cases}$$

I Find the 2×2 matrix X such that $\begin{bmatrix} a_{n+1} \\ b_{n+1} \end{bmatrix} = X \begin{bmatrix} a_n \\ b_n \end{bmatrix}$

II Let $A = \begin{bmatrix} -6 & 5 \\ -5 & 4 \end{bmatrix}$. Calculate $\det(A)$ and A^{-1} .

III Show that $X = A \begin{bmatrix} 2 & 0 \\ 0 & 5 \end{bmatrix} A^{-1}$.

IV By hand, find s_{101} using parts (I)-(III).

Hint: $\begin{bmatrix} 2 & 0 \\ 0 & 5 \end{bmatrix}^{100} = \begin{bmatrix} 2^{100} & 0 \\ 0 & 5^{100} \end{bmatrix}$ and do not calculate 2^{100} or 5^{100} .

Question 3

Denote the number of ways to partition an n -element set into k disjoint non-empty subsets by $S(n, k)$. For example, $S(3, 2) = 3$ since there are 3 ways to partition $\{1, 2, 3\}$ into 2 disjoint non-empty subsets:

- $\mathcal{P}_1 = \{\{1\}, \{2, 3\}\}$
- $\mathcal{P}_2 = \{\{2\}, \{1, 3\}\}$
- $\mathcal{P}_3 = \{\{3\}, \{1, 2\}\}$

Furthermore, let $X = \{x_1, x_2, \dots, x_n\}$ and $Y = \{y_1, y_2, \dots, y_k\}$ be finite sets for some $n, k \in \mathbb{N}$. We will investigate the number of surjective functions from X to Y .

A Calculate $S(4, 3)$ by finding all possible partitions of $\{1, 2, 3, 4\}$ into 3 disjoint non-empty subsets.

B Prove that $S(n, k) = S(n - 1, k - 1) + kS(n - 1, k)$ for $0 < k < n$.

Hint: Consider all possible partitions of $\{1, 2, \dots, n\}$ into k disjoint non-empty subsets and whether $\{n\}$ is an element of the partition or not.

C Prove that the number of surjective functions from X to Y is $k!S(n, k)$.

Hint: A surjective function $f: X \rightarrow Y$ gives rise to a partition of X given by

$$\left\{ \{x \in X \mid f(x) = y\} \mid y \in Y \right\} = \left\{ \{x \in X \mid f(x) = y_1\}, \{x \in X \mid f(x) = y_2\}, \dots, \{x \in X \mid f(x) = y_k\} \right\}.$$

You should also explain why this is the case.

D Suppose you and your classmate have a machine that generates functions from X to Y , so that each function has an equal likelihood of being generated. Suppose your classmate has calculated that $S(4, 2) = 7$. When $n = 5$ and $k = 3$, calculate the probability that the function generated by the machine is surjective.

Question 4

- A Recall that a byte is a binary string of 8 bits. How many bytes contain at least five 1's and one 0?
- B A bank requires a password for you to access your account. The password is a sequence of 12 characters that contains exactly
- 4 lower case alphabetical letters,
 - 2 upper case alphabetical letters,
 - 4 decimal digits and
 - 2 special characters from the set $\{ @, \#, \$, \% \}$.

Note that you are allowed to have repeated characters. Let X denote the set of all possible bank passwords.

For security reasons, the bank does not store your password (imagine what would happen if the file containing all passwords was hacked!). Instead, the bank stores a k -digit PIN (a sequence of k decimal digits) for some $k \in \mathbb{N}$. Let Y be the set of all k -digit PINs. The bank computes such a PIN from your password via a function $f: X \rightarrow Y$. When you enter your password into its system, the bank verifies your password by evaluating f and checking the output against its records.

The **clash score** N of f is given by the number:

$$N = \max_{y \in Y} |\{x \in X \mid f(x) = y\}|$$

What is the least value of k that may give a clash score of no more than 10^{15} ?

Hint: You will need to consider $|X|$, $|Y|$, a property that f will have to allow you to find the least value of k and use an appropriate counting principle from lectures.