Final Report

Discrete Structures

Regulations

You should solve and submit this report to your elearning account within 14 days, from the beginning of May 21st, 2024, to the end of Jun 3rd, 2024. Late submission is not accepted.

This is an group final report. Number of students in a group can not be more than 3

In the test, there are questions that need to be customized according to a student ID. Only the smallest student ID in your group will be used for this purpose. For example, in group of 3 students, said 52200123, 52200136 and 52201001, then only 52200123 are used.

Students need to submit a compressed file named with your Student IDs, eg. 52200123_52200136_52201001.zip/rar, including this structure:

- The document file is in Word format (.doc/docx), named by your Student IDs, eg. 52200123_52200136_52201001.docx, using our faculty's format, from 25 to 35 pages.
    - The tasks of each member and self-evaluation of your group should be declared at the end of this report.
    - English is required for high-quality classes. Format violations will cost from 10% to 50% of your total scores.
    - Any case of plagiarism will get 0.
- The Python source code files are named by your Student ID and Task Number, eg. 52200123_52200136_52201001_8.py and 52200123_52200136_52201001_9.py.

Question 1: Euclid's algorithm and Bezout's identity

a. Using Euclid's algorithm to calculate $gcd(2024, 1000 + m)$ and $lcm(2024, 1000 + m)$, where m is the last 3 digits of your student ID. For example, if your student ID is 52200**123** then you need to calculate $gcd(2024, 1123)$ and $lcm(2024, 1123)$.

b. Apply above result(s) in to find 5 integer solution pairs (x,y) of this equation:

$$2024x + (1000 + m)y = gcd(2024, 1000 + m)$$

For example, if your student ID is 52000**123** then your equation is:

$$2024x + 1123y = gcd(2024, 1123)$$

Question 2: Recurrence relation

Solve this recurrence relation.

$$a_n = 8.a_{n-1} - 15.a_{n-2}$$

with $a_0 = 5$ and $a_1 = m$,

where m is the last 2 digits of your student ID. For example, if your student ID is 52200123 then $a_1 = 23$.

Question 3: Set

a. Create a set Γ of characters from your case-insensitive non-diacritical full name. For example, the set corresponding with "Tôn Đức Thắng" is Δ = {A, C, D, G, H, N, O, T, U}.

b. Find the union, intersect, non-symmetric difference, and symmetric difference of Γ and Δ, where Γ and Δ are from question 3a.

Question 4: Relations

Let $\Re$ be a binary relation defined on 2 integers as follow:

$$\forall a, b \in \mathrm{N}\ (\mathrm{aRb} \leftrightarrow m | (a.b))$$

where m is the last 2 digits of your student ID.

For example, if your student ID is 52200123 then the valid binary relation is

$$\forall a, b \in \mathrm{N}\ (\mathrm{aRb} \leftrightarrow 23 | (a.b))$$

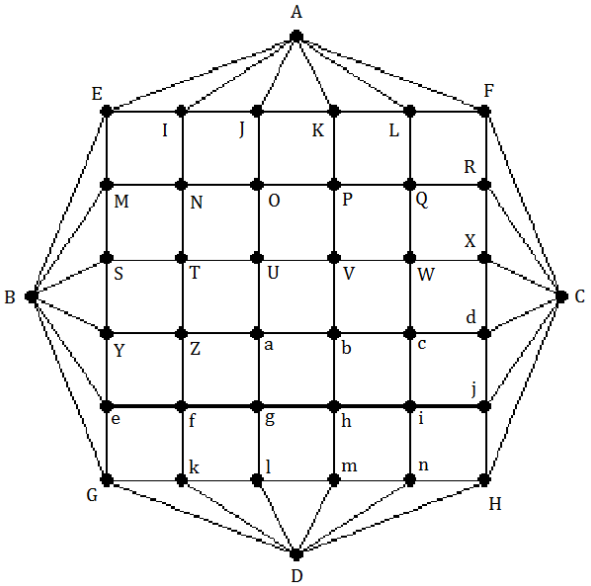
Is R reflexive, symetric, anti-symetric, transitive? Prove your answer.

Question 5: Kruskal's algorithm

Propose a solution for circuit-checking in Kruskal's algorithm. Give an example.

Question 6: Eulerian circuit

a. Does the following graph have an Eulerian circuit or Eulerian path? Why?



b. Study and present your knowledge about Hierholzer's algorithm to find an Eulerian circuit.

c. If the graph has an Eulerian circuit, use Hierholzer's algorithm to find an Eulerian circuit of that graph when the initial circuit R1 is:

i. If $\overline{abcd}$ % 4 = 0 then R1 is EINME

ii. If $\overline{abcd}$ % 4 = 1 then R1 is abhga

iii. If $\overline{abcd}$ % 4 = 2 then R1 is UVbaU

iv. If $\overline{abcd}$ % 4 = 3 then R1 is XCdX

Where $\overline{abcd}$ is the 4-digit number combined by the last 4 digits in your StudentID. For example, Student ID 52201234 has $\overline{abcd}$ = 1234.

Question 7: Map coloring

Given this map:

a. Modeling this map by a graph.

b. Color the map (graph) with a minimum number of colors. Present your solution step by step.

Let $\overline{abcd}$ be the 4-digit number combined by the last 4 digits in your StudentID. For example, StudentID 52201234 has $\overline{abcd}$ = 1234.

i. If $\overline{abcd}$ % 4 = 0 then start from Bihar.

ii. If $\overline{abcd}$ % 4 = 1 then start from Orissa.

iii. If $\overline{abcd}$ % 4 = 2 then start from Rajasthan.

iv. If $\overline{abcd}$ % 4 = 3 then start from Meghalaya.

Question 8: Finding an Inverse Modulo *n*

- Conduct research on Finding an Inverse Modulo *n* using the extended Euclidean algorithm. Give your own examples.
- Implement a Python program to find an Inverse Modulo *n* using the extended Euclidean algorithm. Related libraries are NOT allowed.
- Test the implemented program using sample data and verify the results. Capture your screen results and explain them in your report document.

Question 9: RSA cryptosystem

- Conduct research on RSA cryptosystem. Understand the mathematical concepts behind the RSA cryptosystem, including prime number generation, modular arithmetic, extended Euclidean algorithm, prime factorization, etc. Give your own examples.
- Implement a Python program to encrypt and decrypt a message with the RSA cryptosystem. Cryptography libraries are allowed.
- Test the implemented RSA cryptosystem using sample messages and verify the results. Capture your screen results and explain them in your report document.
- Analyze the efficiency and security of the implemented RSA cryptosystem.
- Discuss the potential security threats and limitations of the RSA cryptosystem.
- Conclude with recommendations for improving the RSA cryptosystem implementation.

Rubric

Criteria		Scale	1	2	3	Self-evalutaion	Reason
		Score /10	0 score	1/2 score	Full score		
Question 1		1	Do nothing or wrongly.	Correct gcd and lcm, but incorrect solutions of the Bezout's identity.	Correct calculation, detailed explanation.		
Question 2		0.5	Do nothing or wrongly.	Correct calculation but wrong result or conclusion.	Correct calculation, detailed explanation.		
Question 3		0.5	Do nothing or wrongly.	Correct Γ but incorrect operations.	Correct calculation, detailed explanation.		
Question 4		0.5	Do nothing or wrongly.	Correct results but incorrect proofs.	Right results, detailed explanation.		
Question 5		1	Do nothing or wrongly.	Reasonable but indetailed proposion. No illustration.	Reasonable detailed proposion with illustration.		
Question 6		1	Do nothing or wrongly.	a-Correct recognition, right explanation. b,c-Good study but incorrect applications.	a-Correct recognition, right explanation. b,c-Good study, right calculation, detailed explanation.		
Question 7		1	Do nothing or wrongly.	Correct modeling but wrong coloring.	Correct modeling but right coloring.		
Question 8	Theorical research	0.5	Do nothing or wrongly	Not enough details, no	Correct calculations, detailed explanations		

				example, no comment			
	Implementation	0.5	Error	Correct but bad performance	Correct and good performance		
	Test	0.5	No test	Test without verification	Test and verification		
Question 9	Theorical research	0.5	Do nothing or wrongly	Not enough details, no example, no comment	Correct calculations, detailed explanations		
	Implementation	0.5	Error	Correct but bad performance	Correct and good performance		
	Test	0.5	No test	Test without verification	Test and verification		
	Analysis	0.5	Do nothing or wrongly	Not enough details, no example, no comment	Correct, detailed explanations		
	Discussion	0.5	Do nothing or wrongly	Not enough details, no example, no comment	Correct, detailed explanations		
	Recommendation	0.5	Do nothing or wrongly	Not enough details, no example, no comment	Correct, detailed explanations		
Total		10			Result	0	