This exam in TMA4140 Discrete Mathematics has the following structure:

Problem 1:	Logic	10 points
Problem 2:	Sets	10 points
Problem 3:	Functions	10 points
Problem 4:	Boolean algebra	10 points
Problem 5:	Relations	10 points
Problem 6:	Induction	10 points
Problem 7:	Combinatorics	10 points
Problem 8:	Graphs and trees	10 points
Problem 9:	Number theory	10 points
Problem 10:	Finite state machines and automata	10 points
Total:		**100 points**

The answer to every problem requires a detailed argument/computation.

Problem 1 **Logic** (10 points)

a. (3 points) Use a truth table to decide whether $[(\neg p \to q) \wedge (p \to q)] \to q$ is a tautology or a contradiction.

b. (3 points) Write the following proposition in conjunctive normal form (CNF)

$$p \to (q \wedge \neg r).$$

c. (4 points) Use 1st-order logic to write down the definition of surjectivity (onto) for a function $f : X \to Y$ and then form the negation of the statement so that no negation sign is to the left of a quantifier. Express the meaning of the negation in simple words.

Solution.

a. Tautology:

p	q	$\neg p \to q$	$p \to q$	$[(\neg p \to q) \wedge (p \to q)] \to q$
0	0	0	1	1
0	1	1	1	1
1	0	1	0	1
1	1	1	1	1

b. Conjunctive normal form means that the result should be of the form $X \wedge Y$.

$$\begin{aligned} p \to (q \wedge \neg r) &\iff \neg p \vee (q \wedge \neg r) \\ &\iff (\neg p \vee q) \wedge (\neg p \vee \neg r). \end{aligned}$$

c. Surjectivity: $\forall y \in Y \exists x \in X(f(x) = y)$,
Negation:

$$\begin{aligned} \neg(\forall y \in Y \exists x \in X(f(x) = y)) &\iff \exists y \in Y \neg(\exists x \in X(f(x) = y)) \\ &\iff \exists y \in Y \forall x \in X \neg(f(x) = y) \\ &\iff \exists y \in Y \forall x \in X(f(x) \neq y). \end{aligned}$$

Explanation in simple English: There exists an element y in the set Y such that f maps every element x in the set X to a different element than y.

Problem 2 **Sets** (10 points)

a. (3 points) What is the power set of $A := \{\{a, b\}, \{c, d, e\}, \{f\}\}$?

b. (7 points) Let A, B, C be sets. The symmetric difference is defined by $A \triangle B := (A \backslash B) \cup (B \backslash A)$. Use an element argument to show that $A \triangle B = (A \cup B) \backslash (A \cap B)$.

Solution.

a.

$$\begin{aligned} P(A) = \{&\emptyset, \{\{f\}\}, \{\{a, b\}\}, \{\{c, d, e\}\}, \\ &\{\{a, b\}, \{c, d, e\}\}, \{\{a, b\}, \{f\}\}, \\ &\{\{c, d, e\}, \{f\}\}, A\}. \end{aligned}$$

b. Let $x \in (A \setminus B) \cup (B \setminus A)$. Then $x \in A \setminus B$ or $x \in B \setminus A$. If $x \in A \setminus B$, then $x \in A$ and $x \notin B$. If $x \in A$, then $x \in A \cup B$. If $x \notin B$, then $x \notin A \cap B$. Hence $x \in (A \cup B) \setminus (A \cap B)$ if $x \in A \setminus B$. If $x \in B \setminus A$, then $x \in B$ and $x \notin A$. If $x \in B$, then $x \in A \cup B$. If $x \notin A$, then $x \notin A \cap B$. Hence $x \in (A \cup B) \setminus (A \cap B)$ if $x \in B \setminus A$. Therefore $(A \setminus B) \cup (B \setminus A) \subseteq (A \cup B) \setminus (A \cap B)$.

Conversely, let $y \in (A \cup B) \setminus (A \cap B)$. Then $y \in (A \cup B)$ and $y \notin (A \cap B)$. If $y \in A \cup B$, then $y \in A$ or $y \in B$. If $y \in A$ and $y \notin A \cap B$, then $y \notin B$. Hence $y \in A \setminus B$ if $y \in A$ and $y \notin A \cap B$. If $y \in B$ and $y \notin A \cap B$, then $y \notin A$. Hence $y \in B \setminus A$ if $y \in B$ and $y \notin A \cap B$. Therefore $(A \cup B) \setminus (A \cap B) \subseteq (A \setminus B) \cup (B \setminus A)$.

We conclude that $(A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$.

Problem 3 Functions (10 points)

a. (3 points) Consider sets $A = \{a, b, c\}$, $B = \{1, 2, 3, 4\}$, and $C = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ and the functions

$$f_1 = \{(a, 2), (b, 3), (c, 1)\} \qquad \text{and} \qquad f_2 = \{(1, \alpha_2), (2, \alpha_2), (3, \alpha_4), (4, \alpha_1)\}.$$

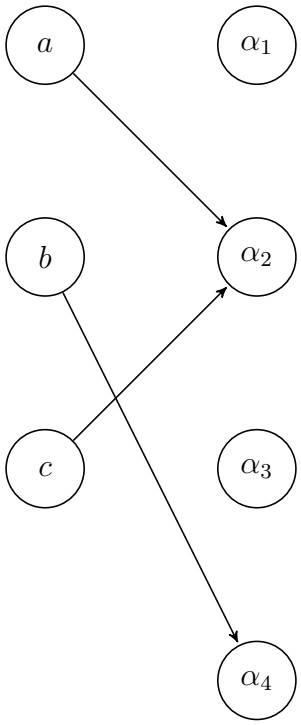
Write down the composition $f_2 \circ f_1$ as a set of ordered pairs and draw its arrow diagram.

b. (7 points) Let m be an odd integer, that is, $m = 2l + 1$ for some integer l. Show that

$$\lfloor \frac{m^2}{4} \rfloor = \Big(\frac{m-1}{2}\Big)\Big(\frac{m+1}{2}\Big).$$

Solution.

a. $f_2 \circ f_1 = \{(a, \alpha_2), (b, \alpha_4), (c, \alpha_2)\}$.



b.

$$\begin{aligned}\lfloor\frac{m^2}{4}\rfloor =&\lfloor\frac{(2l+1)^2}{4}\rfloor\\ =&\lfloor\frac{4l^2+4l+1}{4}\rfloor\\ =&\lfloor l^2+l+\frac{1}{4}\rfloor\\ =&l^2+l\\ =&l(l+1)\\ =&\frac{m-1}{2}\cdot\frac{m+1}{2}.\end{aligned}$$

Problem 4 Boolean algebra (10 points)

Consider the notions of least common multiple (lcm) and the greatest common divisor (gcd). Let $S=\{1,2,3,6\}$ and define the binary operations $x+y:=\text{lcm}(x,y)$ and $x\cdot y:=\gcd(x,y)$ and the unary operation $\overline{x}:=6/x$. Show that $(S,+,\cdot,^{-},1,6)$ is a Boolean algebra.

Solution. Denote the Boolean algebra by B. The axioms are the following:

Commutativity:	$(\forall x,y\in B)(x+y=y+x \text{ and } x\cdot y=y\cdot x)$
Identity axioms:	$(\forall x\in B)(x+0=x \text{ and } x\cdot 1=x)$
Complement axioms:	$(\forall x\in B)(x+\overline{x}=1 \text{ and } x\cdot\overline{x}=0)$
Distributivity of multiplication over addition:	$(\forall x,y,z\in B)(x\cdot(y+z)=x\cdot y+x\cdot z)$
Distributivity of addition over multiplication:	$(\forall x,y,z\in B)(x+y\cdot z=(x+y)\cdot(x+z))$

We check the axioms:

- Commutativity follows from $\text{lcm}(x,y)=\text{lcm}(y,x)$ and $\gcd(x,y)=\gcd(y,x)$.
- Additive identity: $x+1=\text{lcm}(x,1)=x$. Multiplicative identity: $x\cdot 6=\gcd(x,6)=x$.
- Additive complement: $x+\bar{x}=\text{lcm}(x,6/x)=x\cdot\frac{6}{x}=6$, because x and $\frac{6}{x}$ does not have any non-trivial factors in common.
- Multiplicative complement: $x\cdot\bar{x}=\gcd(x,6/x)=1$ because x and $\frac{6}{x}$ does not have any non-trivial factors in common.

- Distributivity: Note that any element in S can be written as $x = 2^i 3^j$, with $i, j \in \{0, 1\}$. Let $x = 2^{i_x} 3^{j_x}, y = 2^{i_y} 3^{j_y}, z = 2^{i_z} 3^{j_z}$, then:

$$\begin{aligned} x(y+z) =& \gcd(x, \operatorname{lcm}(y, z)) \\ =& \gcd(x, 2^{\max(i_y, i_z)} 3^{\max(j_y, j_z)}) \\ =& 2^{\min(i_x, \max(i_y, i_z))} 3^{\min(j_x, \max(j_y, j_z))} \\ =& 2^{\max(\min(i_x, i_y), \min(i_x, i_z))} 3^{\max(\min(j_x, j_y), \min(j_x, j_z))} \\ =& \operatorname{lcm}(\gcd(x, y), \gcd(x, z)) \\ =& xy + xz, \end{aligned}$$

and

$$\begin{aligned} x + yz =& \operatorname{lcm}(x, \gcd(y, z)) \\ =& 2^{\max(i_x, \min(i_y, i_z))} 3^{\max(j_x, \min(j_y, j_z))} \\ =& 2^{\min(\max(i_x, i_y), \max(i_x, i_z))} 3^{\min(\max(j_x, j_y), \max(j_x, j_z))} \\ =& \gcd(\operatorname{lcm}(x, y), \operatorname{lcm}(x, z)) \\ =& (x + y)(x + z). \end{aligned}$$

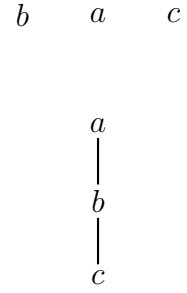
Problem 5 **Relation** (10 points)

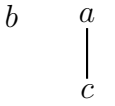
a. (3 points) Draw all possible distinct Hasse diagrams for a poset with 3 elements.

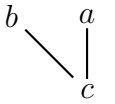
b. (7 points) Draw the Hasse diagram for the poset formed by the divisors of 42.

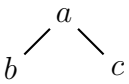
Solution.

a.

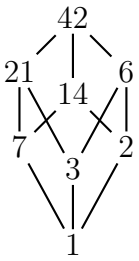








b. $42 = 2 \cdot 3 \cdot 7$:



Problem 6 **Induction** (10 points)

For a positive integer n, define the triangular number $t_n = 1 + 2 + \cdots + n$. Use induction to show that $\sum_{i=1}^{n} t_i = \frac{n+2}{3} t_n$.

Hint: Recall that Carl Friedrich Gauss computed the number t_{100} as $(100 \cdot 101)/2$.

Solution. Base case: $t_1 = \frac{1+2}{3} t_1$.
Inductive step: Suppose that $\sum_{i=1}^{n} t_i = \frac{n+2}{3} t_n$, need to show $\sum_{i=1}^{n+1} t_i = \frac{n+3}{3} t_{n+1}$. We compute:

$$\begin{aligned}
\sum_{i=1}^{n+1} t_i &= t_{n+1} + \sum_{i=1}^{n} t_i \\
&= t_{n+1} + \frac{n+2}{3} t_n \\
&= (n+1) + \frac{n+5}{3} t_n \\
&= \frac{2}{3} t_n + (n+1) + \frac{n+3}{3} t_n,
\end{aligned}$$

now we use the hint $t_n = n \cdot (n+1)/2$ to write:

$$\begin{aligned}
&= \frac{2}{3} \cdot \frac{n}{2} \cdot (n+1) + (n+1) + \frac{n+3}{3} t_n \\
&= (\frac{n}{3} + 1)(n+1) + \frac{n+3}{3} t_n \\
&= \frac{n+3}{3}(t_n + (n+1)) \\
&= \frac{n+3}{3} t_{n+1}.
\end{aligned}$$

Problem 7 **Combinatorics** (10 points)

a. (4 points) What is the coefficient in front of the term x^6y^3 in the polynomial $(3x+4y)^9$?

b. (6 points) We have a bin with 4 balls in different colors: red, green, brown and blue. In how many ways can we

i) (1 point) sample different outcomes?

ii) (2 points) sample different outcomes when we do not sample the red ball last?

iii) (3 points) sample 6 balls from the bin when we do not care about the order we sample, and we put the ball back in the bin after it is sampled?

Solution.

a. Each term in the expansion is of the form $\binom{n}{k} \cdot 3^{n-k} \cdot 4^k \cdot x^{n-k} \cdot y^k$ where n is fixed and k goes from 0 to n. We have $n = 9$ and $k = 3$ for the term we are interested in. It follows that the coefficient is $\binom{9}{3} \cdot 3^6 \cdot 4^3 = 84 \cdot 729 \cdot 64 = 3919104$.

b. i) There are 4 options for the first ball, 3 options for the second ball, 2 option for the third ball, and 1 option for the last ball. We have $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$ ways to sample different outcomes.

ii) If the red ball is not the last sample, it must be the first, second or third. In each case we have $3! = 6$ ways to sample the other three balls, so we have $3 \cdot 6 = 18$ different outcomes when the red is not last.

iii) This is an unordered sampling with repetition with $n = 4$ balls and $k = 6$ samples. This can be visualized with 3 walls ($|$), for example as *red*$|$*green*$|$*brown*$|$*blue*, and 6 stars ($*$), and we get samples of the form $******|\,|\,|$ or $*|**|**|*$ and so on. There are $\binom{n+k-1}{k}$ possible outcomes, and we get that there is $\binom{9}{6} = \frac{9!}{6!\cdot 3!} = \frac{9\cdot 8\cdot 7}{6} = 84$ distinct combinations.

Problem 8 Graphs & trees (10 points)

a. (4 points) Let G be a graph with vertices $V = \{1, 2, 3, 4, 5\}$. Draw the graph of the following adjacency matrix, where an index (i, j) in the matrix is 0 if there is no edge from vertex i to vertex j and 1 if there is an edge. Is G directed or undirected? Is G a simple graph or a multigraph?

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

b. (6 points) Does the graph have

i) (1 point) an Euler trail?

ii) (1 point) an Euler circuit?

iii) (2 points) a Hamiltonian path?

iv) (2 points) a Hamiltonian cycle?

Solution.

a. See drawing in the figure. The graph G is directed since the matrix is not symmetric, and hence, some edges are only going from vertex i to vertex j but not from vertex j to vertex i. The graph is simple since there are no loops and no parallel edges, which we can see from the fact that all of the elements on the diagonal is 0 and that no entry is greater than 1.

b. i) No, for example because vertex 1 has 4 outgoing edges but no incoming edges, so it is impossible to cross all edges in one trail.

ii) No, of the same reason. This can also be seen since each vertex needs equal number of in and out edges, which we do not have.

iii) Yes. But how do we find it? All edges connected to 1 goes out, so this must be the starting point in case a Hamiltonian path exists. All edges edges connected to 5 goes in, so this must be the final vertex. There is no edge from 2 to 3 and no edge from 4 to 2 or 3, and hence, the only possible Hamiltonian path is $1 \to 3 \to 2 \to 4 \to 5$.

iv) No. There is only one possible Hamiltonian path, and it goes from 1 to 5, but there is no edge between 5 and 1, so there can not exist any Hamiltonian cycles.

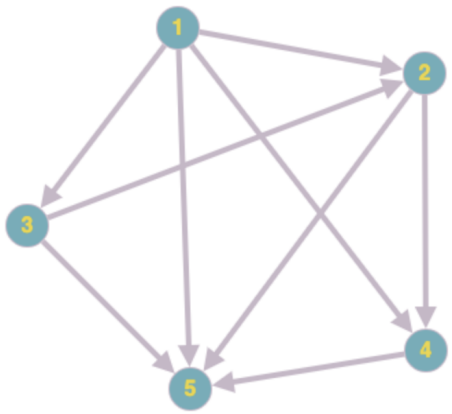


Figure 1: The graph given by the adjacency matrix in problem 8.

Problem 9 **Number theory** (10 points)

a. (4 points) What does Euler's theorem say? Compute $134^{36362} \pmod{675}$.

b. (6 points) Find all integer solutions x to the following system of congruences:

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 4 \pmod{7} \\ x &\equiv 5 \pmod{8} \end{aligned}$$

Solution.

a. Euler's theorem says that if a and n are relatively prime positive integers then $a^{\varphi(n)} \equiv 1 \pmod{n}$, where φ is Eulers phi-function saying how many positive integers smaller or equal to n that are relatively prime to n. We observe that 675 is divisible by small primes and find the factorization $675 = 3^3 \cdot 5^2$. We also observe that 134 is not divisible by 3 or 5. Then, $\varphi(n) = (3^3 - 3^2)(5^2 - 5) = 360$ and, furthermore, $134^{360} \equiv 1 \pmod{675}$ and we have that $36362 = 101 \cdot 360 + 2$. Solution: $134^{36362} \equiv 134^2 = 17956 \equiv 406 \pmod{675}$.

b. All moduli are relatively prime, so there exists a unique solution modulo $3 \cdot 5 \cdot 7 \cdot 8 = 840$. The solution is $x \equiv \sum_{i=1}^{r} a_i M_i k_i \pmod{M}$ where r is the number of congruences of the form $x \equiv a_i \pmod{m_i}$, $M = m_1 \cdot \cdots \cdot m_r$ is the product of all individual moduli, $M_i = M/m_i$, and k_i is the inverse of M_i modulo m_i. We compute $k_1 \equiv 280^{-1} \equiv 1 \pmod 3$ and $k_2 \equiv 168^{-1} \equiv 3^{-1} \equiv 2 \pmod 5$ and $k_3 \equiv 120^{-1} \equiv 1 \pmod 7$, and $k_4 \equiv 105^{-1} \equiv 1 \pmod 8$. Solution: $x \equiv 2 \cdot 280 + 3 \cdot 168 \cdot 2 + 4 \cdot 120 + 5 \cdot 105 = 2573 \equiv 53 \pmod{840}$.

Problem 10 Finite state machines & automata (10 points)

a. (4 points) Draw the transition diagram of the finite state machine F with input $I = \{a, b, c\}$, output $O = \{0, 1\}$ and states $S = \{s_0, s_1, s_2\}$ (initial state is s_0) and the following transition table. What is the output for the input string *aabbcc*?

F	η			μ		
	a	b	c	a	b	c
s_0	s_0	s_1	s_2	0	1	0
s_1	s_1	s_1	s_0	1	1	1
s_2	s_2	s_1	s_0	1	0	0

b. (6 points) Draw the transition diagram of an automaton with five states and input $I = \{a, b\}$ accepting strings containing the sub-string: *abba*.

Solution.

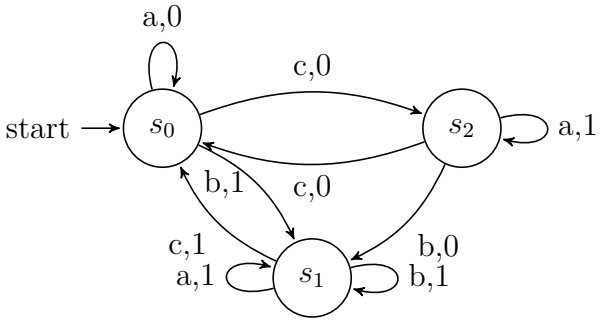


Figure 2: Solution to Problem 10.a. Output for the string *aabbcc* is 001110.

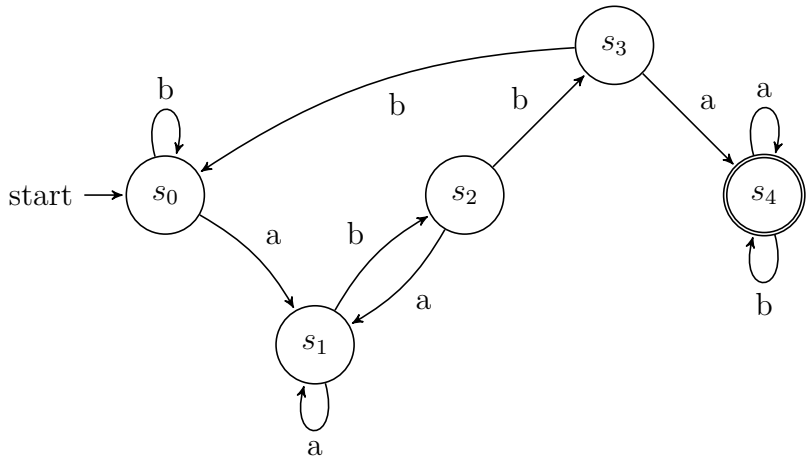


Figure 3: Solution to Problem 10.b.