Namn eller kod *Name or Code*		Grupp *Group*
Personnummer *Civic registration number*	Program *Programme*	Antagningsår *Admission year*

Skriftlig tentamen i *Written examination in*	Kurskod *Course code*
Diskret Matematik	MA112B

Datum *Date*	Skrivtid *Examination time*
2024-03-22	9:00-14:00

Lärare *Teacher*

Niklas Gador, email: niklas.gador@hkr.se , tel. 072 211 19 10

Tillåtna hjälpmedel *Permitted aid*

a calculator, a dictionary

Övrigt *Further information*

Write your name on the top of every page you submit. You must have a minimum of 1 point on each question to pass.

Uppgift *Question*	Poäng *Points*	Resultat *Result*
1	3	
2	3	
3	3	
4	3	
5	3	
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
Max poäng *Max no of points*	15	
Summa *Sum*		
Betyg *Grade*		

Inlämningstid *Submit time*	
Legitimation *ID*	
Antal inlämnade blad *No. of submitted sheets*	
Kontrollerat av student *Checked by student*	
Kontrollerat av skrivvakt *Checked by invigilator*	

Betygsgränser *Grade limits*

			ECTS
G *Pass*	3	7-9	A
VG *Pass w Distinction*	4	10-12	B
	5	13-15	C
			D
			E

Utkvitterad *Received*	
Datum *Date*	

Question 1

Logic

a) Show that $(p \to \sim q) \vee (p \wedge q)$ is a tautology.

b) Show that $\sim (p \wedge \sim q) \vee (q \wedge r)$ is logically equivalent to $\sim p \vee q$.

c) Use the laws of logic to simplify the expression $\sim (p \to q) \vee \sim q$. You have to note which law you used in every step to get points.

Question 2

Number representation and digital logic circuits

a) Perform the following computations in binary arithmetic (Show how you perform the computations):

i. $11010111_2 + 00110010_2$

ii. $10111001_2 - 01100011_2$

b) Use 8-bit two´s complements to compute the following expressions:

i. $45 - 58$

ii. $-13 + 19$

c) Consider the input/output table below.

i. Construct a Boolean expression with this table as its truth table.

ii. Design a digital logic circuit for the Boolean expresssion.

P	Q	R	S (Output)
1	1	1	0
1	1	0	1
1	0	1	0
1	0	0	0
0	1	1	0
0	1	0	1
0	0	1	0
0	0	0	1

Question 3

Sets and relations

a) Let $A = \{1, \{1\}, 2, 3, \{4\}\}$. Determine, and explain in your own words, which of the following statements are true:

i. $\{1\} \subseteq A$

ii. $\{1\} \in A$

iii. $\{1, 2, 4\} \subseteq A$

iv. $4 \in A$

b) Illustrate the set, $((A \cup B) \cap C^c) \cup (B \cap C)$ using a series of Venn diagram. (Note! C^c is the complement of C).

c) Use the properties of Sets to show that $A \cup (A^c \cap B) = A \cup B$. You need to explain each step.

Question 4

Relations and Functions

a) Let $A = \{1, 2, 3, 4\}$ and $B = \{1, 5, 6, 7\}$ and define a relation R from A to B as follows: Given any $(x, y) \in A \times B$, $(x, y) \in R$ means that $(x - y)/3$ is an integer.

i. State explicitly which ordered pairs are in R.

ii. Draw an arrow diagram for R.

b) Let A be the following set $A = \{1, 2, 3, 4, 5, 6\}$. A relation S on A is defined as follows: For every $x, y \in A$, x is related to y if x/y is an integer.

Determine if the relation S as defined above is:

i. reflexive

ii. symmetric

iii. transitive

Hint:

(a) R is *reflexive* if, and only if, for every $x \in A, xRx$.

(b) R is *symmetric* if, and only if, for every $x, y \in A$, if xRy then yRx.

(c) R is *transitive* if, and only if, for every $x, y, z \in A$, if xRy and yRz then xRz.

c) Let A be the set $A = \{0, -1, -2, -3\}$ and B be the set $B = \{0, 1, 2, 3\}$. A function f is defined as follows $f : A \to B, f(x) = (x^2 + 2x + 7) \mod 4$.

i. Is f one-to-one?

ii. Is f onto?

iii. Does f^{-1} exist?

Motivate your answers!

Question 5

Number theory and Cryptography

a) Let $GCD(a, b)$ be the greatest common divisor of a and b. What is $GCD(6370, 5183)$?

b) You have been given the following public key of an RSA public key system, $n = 221$, $e = 11$. Encrypt the message $m = 10$. (Hint! $c = m^e \mod n$). Show all calculations.

c) Given the same RSA publoc key system as in **b)** find the decryption key d and decrypt the ciphertext $c = 5$.
(Hint! $ed \mod (p-1)(q-1) = 1$.)

APPENDIX – Formulas and laws

Laws of logic

Law(s)		*Name*
$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$		Equivalence law
$p \rightarrow q \equiv \neg p \vee q$		Implication law
$\neg\neg p \equiv p$		Double negation law
$p \wedge p \equiv p$	$p \vee p \equiv p$	Idempotent laws
$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$	Commutative laws
$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$	Associative laws
$p \wedge (q \vee r) \equiv$ $(p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv$ $(p \vee q) \wedge (p \vee r)$	Distributive laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$	$\neg(p \vee q) \equiv \neg p \wedge \neg q$	de Morgan's laws
$p \wedge \mathrm{T} \equiv p$	$p \vee \mathrm{F} \equiv p$	Identity laws
$p \wedge \mathrm{F} \equiv \mathrm{F}$	$p \vee \mathrm{T} \equiv \mathrm{T}$	Annihilation laws
$p \wedge \neg p \equiv \mathrm{F}$	$p \vee \neg p \equiv \mathrm{T}$	Inverse laws
$p \wedge (p \vee q) \equiv p$	$p \vee (p \wedge q) \equiv p$	Absorption laws

Boolean axioms

▶ $x + y = y + x$	$x \times y = y \times x$	commutative axioms
▶ $x + (y + z) = (x + y) + z$	$x \times (y \times z) = (x \times y) \times z$	associative axioms
▶ $x + (y \times z) =$ $(x + y) \times (x + z)$	$x \times (y + z) =$ $(x \times y) + (x \times z)$	distributive axioms
▶ $x + 0 = x$	$x \times 1 = x$	identity axioms
▶ $x + x' = 1$	$x \times x' = 0$	inverse axioms

The operations $+$, $\times$ and $'$ are called *addition*, *multiplication* and *complementation* respectively.

Boolean laws

▶ $x'' = x$		double complement law
▶ $x + x = x$	$x \times x = x$	idempotent laws
▶ $(x + y)' = x' \times y'$	$(x \times y)' = x' + y'$	de Morgan's laws
▶ $x + 1 = 1$	$x \times 0 = 0$	annihilation laws
▶ $x + (x \times y) = x$	$x \times (x + y) = x$	absorption laws
▶ $0' = 1$	$1' = 0$	complement laws