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*
2023-08-25	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, angle ruler

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

Number representation and the linear congruential generator

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

i. $111001_2 \times 10111_2$

ii. $101110001_2/110000_2$

b) Convert the following decimal numbers into binary number representation:

i. The decimal number 747.86 to a binary number, with 4 binary digits after the fractional point.

ii. The decimal number -67 to a binary number, using a 2-complement representation with 8 bits.

c) Assume that we have a linear congruential generator ($ax_{i-1} + c \mod m$), with $a = 5$, $c = 7$, and $m = 17$. Write the first 6 integers in the sequence (not including the initial seed) that will be generated if the seed is 7.

Question 2

Sets and relations

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

i. $\{2\} \subseteq A$

ii. $\{2\} \in A$

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

iv. $3 \in A$

b) Illustrate the set, $((A \cap B) \cup \overline{B}) \cap (A \cap \overline{C})$ using a series of Venn diagram.

c) Let A be the following set $A = \{0, 1, 2, 3, 4\}$. A binary relation R on the set A is defined as follows: x is related to y if $|x - y| < 2$, i.e., the absolute value of the difference between x and y is smaller than 2.

Determine if the relation R as defined above is:

i. reflexive

ii. symmetric

iii. antisymmetric

iv. transitive

Hint:

(a) R is *reflexive* if xRx for all $x \in A$..

(b) R is *irreflexive* if there are no elements x of A for which xRx.

(c) R is *symmetric* if xRy implies yRx, for all $x, y \in A$.

(d) R is *antisymmetric* if xRy and yRx then $x = y$, for all $x, y \in A$.

(e) R is *transitive* if xRy and yRz imply xRz, for all $x, y, z \in A$.

Question 3

Logic and functions

a) Show that $(\neg p \to q) \wedge (\neg p \wedge \neg q)$ is a contradiction.

b) Let the functions f, g, and h be defined as follows:

$$f : \mathbf{R} \to \mathbf{R}, f(x) = 3x - x$$
$$g : \mathbf{R} \to \mathbf{R}, g(x) = x^2 + x$$
$$h : \mathbf{R} \to \mathbf{R}, h(x) = -(x + 1)^2$$

Calculate the following function compositions:

i. $f \circ g$

ii. $h \circ f$

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

i. Is f one-to-one?

ii. Is f onto?

iii. Does f^{-1} exist?

Motivate your answers!

Question 4

Boolean Algebra

a) Use the axioms and laws of Boolean Algebra to simplify the expression $(xx' + yx)' + y$. You have to note which law you used in every step to get points.

b) The following Boolean function, $f(x, y, z, w)$, where x, y, z, w are Boolean variables (can only take values 0 or 1), is defined according to the Truth Table,

x	y	z	w	$f(x, y, z, w)$
0	0	0	0	d
0	0	0	1	d
0	0	1	0	d
0	0	1	1	1
0	1	0	0	d
0	1	0	1	1
0	1	1	0	1
0	1	1	1	d
1	0	0	0	0
1	0	0	1	0
1	0	1	0	d
1	0	1	1	d
1	1	0	0	0
1	1	0	1	0
1	1	1	0	0
1	1	1	1	d

The d's stand for 'don't care', and can each be set to either a 0 or a 1, in order to get the minimum expression for f.

Use the Karnaugh map below to find a minimum expression for f !

Karnaugh Map:

	zw	$z'w$	$z'w'$	zw'
xy				
$x'y$				
$x'y'$				
xy'				

c) Lets obtain a boolean function, $f(x, y, z)$, for the operation:
f = ('sum bit' OR 'carry bit') in a 'full adder' , that is
$f = (f1 \text{ OR } f2)$ is 0 when both $f1$ and $f2$ are 0, and 1 otherwise

A full adder takes 3 input Boolean variables, (x, y, z), and makes two separate output functions, $f1(x, y, z)$ and $f2(x, y, z)$.

The task of a full adder is to make a binary addition of three input binary variables, x, y, z, e.g.

$$\begin{array}{r} 0 \\ 1 \\ +\ 1 \\ \hline 1\ 0 \end{array} \quad \text{or} \quad \begin{array}{r} 1 \\ 1 \\ +\ 1 \\ \hline 1\ 1 \end{array} \quad \text{or} \quad \begin{array}{r} 0 \\ 0 \\ +\ 0 \\ \hline 0\ 0 \end{array} \quad \cdots$$

In general,

$$\begin{array}{cc} & x \\ & y \\ + & z \\ \hline f2 & f1 \end{array}$$

i. Make a Truth Table for $f(x,y,z) = f1(x,y,z)\text{OR}f2(x,y,z)$, for all possible combinations of x, y, z (8 combinations), following the expected result of binary addition of three digits.

ii. Use a Karnaugh map to find a simplified expression (if possible) for the function $f(x,y,z)$.

Karnaugh Map:

	yz	$y'z$	$y'z'$	yz'
x				
x'				

Question 5

Number Theory

a) Use the Euclidean algorithm and find the greatest common divisor $d = \gcd(a,b)$ and the least common multiple $m = \text{lcm}(a,b)$ when $a = 1235$ and $b = 1729$.

b) Use the Euclidean algorithm steps to find ALL the integer solutions of the equation,

$$13x + 216y = 1$$

c) You have been given the following public key of an RSA public key system, $n = 247$, $e = x = 17$.

i. Encrypt the message $m = 4$. (Hint! $c = m^e \mod n$).

ii. Find the decryption key d and decrypt the ciphertext $c = 3$. (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