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*: 2023-03-24	Skrivtid *Examination time*: 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

Number representation and the linear congruential generator

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

i. $11101_2 \times 10011_2$

ii. $1111011_2/110000_2$

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

i. The decimal number 17.36 to a binary number, with 5 binary digits after the fractional point.

ii. The decimal number -34 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 $a = 3$, $c = 5$, and $m = 16$. Write the sequence that will be generated if the seed is 1, until it repeats itself.

Question 2

Sets and relations

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

i. $\{3\} \subseteq A$

ii. $\{3\} \in A$

iii. $\{2, \{3\}\} \subseteq A$

iv. $4 \in A$

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

c) Let A be the following set $A = \{0, 1, 2, 3, 4, 5\}$. A binary relation R on the set A is defined as follows: x is related to y if $(x + y) \mod 6 = 2$, i.e., the sum of x and y modulo 6 is 2.

Determine if the relation R as defined above is:

i. reflexive

ii. irreflexive

iii. symmetric

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 *transitive* if xRy and yRz imply xRz, for all $x, y, z \in A$.

Question 3

Logic and functions

a) Show that $((q \to r) \vee (q \wedge \neg r)) = T$.

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

$$f : \mathbf{R} \to \mathbf{R}, f(x) = x + 7$$
$$g : \mathbf{R} \to \mathbf{R}, g(x) = \tfrac{1}{x}$$
$$h : \mathbf{R} \to \mathbf{R}, h(x) = -(x + 1)^2$$

Calculate the following function compositions:

i. $f \circ g$

ii. $h \circ g$

c) A discrete function f has the domain $X = \{\frac{1}{2}, 1, \frac{3}{2}, 2\}$ and the codomain $Y = \{\frac{5}{2}, 2, \frac{13}{6}\}$. The function f is defined as follows $f : X \to Y, f(x) = x + \frac{1}{x}$.

i. Is f one-to-one?

ii. Is f onto?

iii. Does f^{-1} exist?

Motivate your answers!

Question 4

Boolean Algebra

a) 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	1
0	0	1	0	1
0	0	1	1	0
0	1	0	0	0
0	1	0	1	d
0	1	1	0	1
0	1	1	1	1
1	0	0	0	0
1	0	0	1	0
1	0	1	0	d
1	0	1	1	d
1	1	0	0	1
1	1	0	1	0
1	1	1	0	1
1	1	1	1	0

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'				

b) Write the Boolean expression $x(yz)'$ in Disjunctive Normal form.

c) Make a digital circuit of the Boolean expression $(xy)' + z + (x + w)'$

Question 5

Number Theory

a) Use the Euclidean algorithm and find the greatest common divisor $d = \gcd(a, b)$ when $a = 231$ and $b = 165$.

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

$$5x + 72y = 1$$

c) You have been given the following public key of an RSA public key system, $n = 91$, $e = x = 5$.

i. Encrypt the message $m = 2$. (Hint! $c = m^e \mod n$).

ii. Find the decyption key d and decrypt the ciphertext $c = 7$.
(Hint! $ed \mod (p-1)(q-1) = 1$, and $m = c^d mod n$.)

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