HAND IN
Answers recorded
in question paper

QUEEN'S UNIVERSITY
FACULTY OF ARTS AND SCIENCE
SCHOOL OF COMPUTING

CISC-203*
DISCRETE MATHEMATICS FOR COMPUTING SCIENCE

TEST 1
October 2005

Professor Selim G. AKL

Please write your answer to each question only in the box marked **Answer**.
No questions will be answered by the instructor during the exam.
This is a closed-book exam. No computers or calculators are allowed.
If you are unsure of what is wanted for a particular question,
make a reasonable assumption and write this at the beginning of your answer.
PLEASE NOTE: Proctors are unable to respond to queries about the interpretation
of exam questions. Do your best to answer exam questions as written.

NAME: ____

STUDENT NUMBER: ____________________________

FOR INSTRUCTOR'S USE ONLY

Question 1: ______ / 5

Question 2: ______ / 5

Question 3: ______ / 5

Question 4: ______ / 5

TOTAL: _________ / 20

Question 1: [5 marks]

(a) Let A and B be two sets. Show that

Answer:

(i) $A = A \cap (A \cup B)$

If $x \in A$ (the left-hand side), then clearly $x \in A \cup B$, from which it follows that $x \in A \cap (A \cup B)$ (the right-hand side). This means that $A \subseteq A \cap (A \cup B)$.

On the other hand, if $x \in A \cap (A \cup B)$ (the right-hand side), then certainly $x \in A$ (the left-hand side). This implies that $A \cap (A \cup B) \subseteq A$.

(ii) $A = A \cup (A \cap B)$

If $x \in A$ (the left-hand side), then clearly $x \in A \cup (A \cap B)$ (the right-hand side). This means that $A \subseteq A \cup (A \cap B)$.

Conversely, if $x \in A \cup (A \cap B)$ (the right-hand side), then either $x \in A$ or $x \in (A \cap B)$; in both cases $x \in A$ (the left-hand side). Thus, $A \cup (A \cap B) \subseteq A$.

(b) Let A and B be subsets of the finite universal set U. Show that

$$|\overline{A} \cap \overline{B}| = |U| - |A| - |B| + |A \cap B|.$$

Answer:

$$\begin{aligned}
|\overline{A} \cap \overline{B}| &= |\overline{A \cup B}| \\
&= |U| - |A \cup B| \\
&= |U| - (|A| + |B| - |A \cap B|) \\
&= |U| - |A| - |B| + |A \cap B|
\end{aligned}$$

Question 2: [5 marks]

(a) Determine whether each of the following functions $f\colon \mathbf{Z} \to \mathbf{Z}$ (where $\mathbf{Z}$ is the set of integers) is one-to-one and justify your answer:

Answer:

(i) $f(n) = n^2 + 1$

This function is not one-to-one; thus, for example, $f(1) = f(-1) = 2$.

(ii) $f(n) = \lceil n/2 \rceil$

This function is not one-to-one; thus, for example, $f(1) = f(2) = 1$.

(b) Determine whether each of the following functions $f\colon \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$ is onto, and justify your answer:

Answer:

(i) $f(m, n) = 2m - n$

This function is onto since, for every integer n, $f(0, -n) = n$.

(ii) $f(m, n) = m + n + 1$

This function is onto since, for every integer n, $f(0, n - 1) = n$.

Question 3: [5 marks]

(a) Use the Euclidean algorithm to find gcd(2346,5432).

Answer:

$$\begin{array}{rcrcr} 5432 & = & 2346 \cdot 2 & + & 740 \\ 2346 & = & 740 \cdot 3 & + & 126 \\ 740 & = & 126 \cdot 5 & + & 110 \\ 126 & = & 110 \cdot 1 & + & 16 \\ 110 & = & 16 \cdot 6 & + & 14 \\ 16 & = & 14 \cdot 1 & + & 2 \\ 14 & = & 2 \cdot 7 & + & 0 \end{array}$$

Therefore, gcd(2346,5432) = 2.

(b) Use Fermat's Little Theorem to compute 2^{364} **mod** 7.

Answer:

By Fermat's Little Theorem $2^6 \equiv 1 \pmod 7$. Therefore, $2^{360} = (2^6)^{60} \equiv 1^{60} \equiv 1 \pmod 7$. It follows that $2^{364} = 2^4 \cdot 2^{360} \equiv 16 \cdot 1 \equiv 16 \pmod 7$, and so 2^{364} **mod** $7 = 2$.

Question 4: [5 marks]

(a) Compute the Boolean product of the following two matrices:

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \qquad \text{and} \qquad \mathbf{B} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{bmatrix}.$$

Answer:

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

(b) Let $\mathbf{A} = c\mathbf{I}$, where c is a real number and $\mathbf{I}$ is the $n \times n$ identity matrix, and let $\mathbf{B}$ be an $n \times n$ matrix. Show that $\mathbf{AB} = \mathbf{BA}$.

Answer:

$\mathbf{AB} = c\mathbf{IB} = c\mathbf{B} = c\mathbf{BI} = \mathbf{B}c\mathbf{I} = \mathbf{BA}$