Name: ________________________________ Student Number: ________________________	CISC 203 Discrete Mathematics for Computing Science Test 2 Fall 2011 Professor Mary McCollam

This test is 50 minutes long and there are 40 marks. **Please write in pen and only in the box marked "Answer".**
This is a closed-book exam. No computers or calculators are allowed.

Question1: [10 marks]

Find an inverse of 9 modulo 19. Then solve the congruence $9x \equiv 17 \pmod{19}$**.** Show the steps leading to the solution and give the answer modulo 19.

Answer:

1. Find an inverse of 9 modulo 19: 17
   Steps of Euclid's Algorithm for gcd(19,9): $19 = 9 \cdot 2 + 1$
   $9 = 9 \cdot 1$

   Working backwards through steps to find linear combination of 9 and 19 equal to 1:
   $1 = 19 – 2 \cdot 9$

   So, all integers congruent to -2 modulo 19 are inverses of 9 modulo 19:
   … , -21, -2, 17, 36, …

2. Multiply both sides of congruence by an inverse and solve for x

   $17 \cdot 9x \equiv 17 \cdot 17 \pmod{19}$
   $153x \equiv 289 \pmod{19}$
   $x \equiv 4 \pmod{19}$

   So, all integers congruent to 4 modulo 19 are solutions to the congruence:

   … , -34 ,-15, 4, 23, 42, …

Question 2: [10 marks]

Let $A = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix}$

(a) Find $(A \wedge B) \odot A$

Recall that $\wedge$ denotes the Boolean *meet* operation and $\odot$ denotes the Boolean *product* operation. Show the result of $A \wedge B$, as well as the final result.

$A \wedge B = \begin{matrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{matrix}$ $\quad (A \wedge B) \odot A = \begin{matrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{matrix}$

(b) Let x, n, and m be positive integers (≥1). Provide a recursive algorithm that computes

$x^n \bmod m$

using the identity

$$x^n \bmod m = ((x^{n-1} \bmod m)(x \bmod m)) \bmod m$$

Answer:

procedure power(x, n, m : positive integers)

if n = 1 then power(x, n, m) ← x mod m

else power(x, n, m) ← ((x mod m) • power(x, n – 1, m)) mod m

This method, of course, is inefficient.

Question 3: [10 marks]

(a) Use a direct proof to show that the product of two odd numbers is odd.

Answer:

An odd number is one of the form 2n+1, where n is an integer. We are given two odd numbers, say 2a+1 and 2b+1. Their product is:

$$(2a+1)(2b+1) = 4ab + 2a + 2b + 1$$

$$= 2(2ab + a + b) + 1$$

This last expression shows that the product is odd, since it is of the form 2n+1, with n = 2ab + a + b.

(b) Use ***either*** a proof by contraposition or a proof by contradiction to show that if m and n are integers and mn is even, then m is even or n is even.

Answer:

Either one of the following

Proof by Contraposition: Assume that it is not true that m is even or n is even. Then both m and n are odd. Since the product of two odd numbers is odd (see part a), mn is odd.

We have shown that if it is not true that m is even or n is even, then it is not true that mn is even. Therefore, we have shown that if mn is even, then m is even or n is even.

Proof by Contradiction: Assume that mn is even and that m and n are both odd. Since the product of two odd numbers is an odd number, mn is odd, so we have a contradiction: mn is even and mn is odd.

Therefore, if mn is even, m is even or n is even.

Question 4: [10 marks] Use mathematical induction to prove that

$$n! < n^n, \text{ where } n \text{ is an integer greater than 1.}$$

Recall that the definition of $n!$ is:

$0! = 1$
$(n+1)! = (n+1)(n!)$

Answer:

Basis Step: Show that P(2) is true

When $n = 2$, $2! = 2 < 2^2$

Inductive Hypothesis: Assume that P(k) is true

Assume that $k! < k^k$

Inductive Step: Show that P(k+1) is true

Show that then $(k+1)! < (k+1)^{k+1}$

$(k + 1)! = (k + 1)k!$ by the definition of n!

$< (k + 1) k^k$ by the inductive hypothesis

$< (k + 1)(k + 1)^k$

$= (k + 1)^{k+1}$